目　录

CONTENTS

绪　论

Euler 在 1772 年发现了下列有趣的事实:

当 $x=0, 1, \cdots, 40$ 时, x^2-x+41 均是素数.

这一事实, 与所谓的 Gauss 的类数 1 问题密切相关, 因为我们有下列的命题 A.

命题 A(Rabinovitch[88]) 设无平方因子整数 $D<0$, $D\equiv 1 \pmod 4$. 则当 $x=0, 1, \cdots, \frac{|D|-3}{4}$ 时, $x^2-x+\frac{1+|D|}{4}$ 均表素数的充要条件是虚二次域 $Q(\sqrt{D})$ 的整数环是唯一分解的, 即 $Q(\sqrt{D})$ 的类数为 1.

由于虚二次域 $Q(\sqrt{-163})$ 的类数是 1, 所以我们由定理 A 立即得出 Euler 断言的真实性.

同样的, 我们可以有下面的命题 B.

命题 B (陆洪文[46]) 设无平方因子整数 $D=4N^2+1$, 其中正整数 $N>1$. 则当 $x=1, 2, \cdots, N-1$ 时, N^2-x-x^2 均表素数的充要条件是实二次域 $Q(\sqrt{D})$ 的整数环是唯一分解的, 即 $Q(\sqrt{D})$ 的类数为 1.

由于 $N=13$ 时, $D=677$, 而 $Q(\sqrt{677})$ 的类数为 1, 所以我们有下列事实:

当 $x=1, 2, \cdots, 12$ 时, $169-x-x^2$ 均是素数.

这样寻找类数为 1 的二次数域是一个既古老又很有意义的问题. 这个问题是 Gauss 提出的. Gauss 在其名著《Disquisitiones Arithmeticae》(《算术研究》, 于 1801 年, Gauss 24 岁时出版)中, 提出下列三个著名的猜想, 它们用现代语言叙述, 即为

1. 当判别式 $D\to-\infty$ 时, 虚二次域 $Q(\sqrt{D})$ 的类数 $h(D)\to$

$+\infty$;

2．正好存在九个类数为1的虚二次域，十八个类数为2的虚二次域和十六个类数为3的虚二次域，等等；

3．存在无穷多个类数为1的实二次域。

1918—1934年间，Hecke[43]，Deuring[13]，Mordell[81]以及Heilbronn[30]等人的工作，完全解决了Gauss的第一个猜想，即有下列的定理C。

定理 C(Hecke-Deuring-Mordell-Heilbronn)

$$h(D)\to+\infty,\ \text{如}\ D\to-\infty,$$

这里D表二次数域$Q(\sqrt{D})$的判别式，$h(D)$为其类数。

在Heilbronn和Linfoot[31] (1934)工作的基础上，K. Heegner[29]、A. Baker[3]和H. Stark[95-96]、[99]的工作，完全解决了Gauss关于类数1和2的虚二次域的猜想，即有下列的定理D。

定理 D(Heegner-Baker-Stark) 分别正好有九个和十八个类数为1和2的虚二次数域，它们的判别式分别是-3，-4，-7，-8，-11，-19，-43，-67，-163（这些的类数为1）和-15，-20，-24，-35，-40，-51，-52，-88，-91，-115、-116，-123，-148，-187，-235，-267，-403，-427（这些的类数为2）。

另外，C.L.Siegel[92] (1935)和Tatuzawa[103] (1951)的工作给出了下面的定理E。

定理 E(Siegel-Tatuzawa) 对任给的正常数$\delta>0$，均存在可以有效计算的正常数C_δ，使得至多除去一个二次数域以外，恒有

$$h(D)R_D>C_\delta|D|^{\frac{1}{2}-\delta}.$$

这里D、$h(D)$分别表示二次数域$Q(\sqrt{D})$的判别式、类数，而R_D是1（对虚二次域）或正则子（对实二次数域）。

关于虚二次域的Gauss类数猜想，最后是由D.Goldfeld[22] (1975)、B.Gross和D.Zagier[23] (1983)的工作解决的，即有下面

的定理 F。

定理 F(Goldfeld-Gross-Zagier) 对判别式为D的虚二次数域$Q(\sqrt{D})$，其类数

$$h(D)>\frac{1}{55}(\log|D|)\prod_{\substack{p\mid|D|\\ p\neq|D|}}\left(1-\frac{[2\sqrt{p}]}{p+1}\right),$$

其中p表素数，$[x]$表x的整数部分。

我们做了参考文献中的 [57] (1986)，上述常数 55 可以改进为 54。

Goldfeld 的想法是利用椭圆曲线理论中的 BSD 猜想，把上述定理的证明归结为找到一条椭圆曲线，它的 Hasse-Weil L-函数在$s=1$处有一个三阶零点。Gross 和 Zagier 花了 7 年的功夫完成了后一任务。

这样下一步的任务，理所当然地转向了关于实二次域的 Gauss 类数猜想(3)。

由上述的 Siegel-Tatuzawa 定理可以看到，实二次域$Q(\sqrt{D})$有关问题的困难还在于它的所谓的正则子$\log\varepsilon_D$，其中ε_D为$Q(\sqrt{D})$的基本单位。

现在关于实二次域方面的结果还非常不完善，即使在小正则子时的情况，也只相当于虚二次域在六十年代以前的水平上，所以还有许多工作可做。现在的状况见第六章。

本书的目的，一方面概述虚二次域方面的卓越成果，另一方面着重叙述实二次域方面的情况。

本书第一章讲述实二次无理数的连分数展开，它的本身似乎非常初等和简单，但是却在关于实二次域的研究中起着非常重要的作用，究其原因，还是上述的正则子在作怪。

第二章讲述二元二次型与二次域的一般理论，这些内容是经典的，例如可见华罗庚的《数论导引》，只有个别的新结果，例如关于某些完全特征和的公式和实二次域的初等类数公式。

第三章讲述极限公式。虚二次域方面的结果是经典的。实二次域方面的结果为以后的研究作了很好的准备。

从第四章起用三章的篇幅讲述Gauss类数问题，其中第四章讲述五十年代以前的工作，包括Euclid域的决定；第五章讲述虚二次域Gauss类数问题的完整解决的详细情况，第六章致力于实二次域的Gauss类数问题，详细地阐述了近年来国内外在这方面的研究成果。

第七章讲述所谓的Hirzebruch和在Hecke算子作用下的变化情况，这也和Gauss类数问题有关，特别是和实二次域正则子的有关猜想密切相关。

希望本书的出版有助于Gauss类数猜想的进一步研究，特别希望能吸引有兴趣的年轻学者来攀登这一个科学高峰。由于本人能力的限制，本书难免出现谬误和遗漏，请读者不吝指教为感。

最后，作者对自己的导师，已故数学大师华罗庚教授表示衷心的感谢和深切的怀念；同时对自己的师长王元教授和谷超豪教授、同门冯克勤教授表示由衷的谢忱，他们仔细地审阅了本书的原稿。

陆洪文

1994.1.

第 1 章

连分数与 Pell 方程

由于实二次域的基本单位为一个 Pell 方程的最小解所确定，而后者又可以用连分数表出，所以连分数对实二次域的研究是一个非常有用的工具。我们在第一节中讲述实二次无理数的连分数展开，包括简单连分数、半单连分数和奇异连分数。在第二节中讲述 Pell 方程和更一般的二元二次不定方程的解。有关的结论都是研究实二次域类数问题的必要的准备工作。

§1 实二次无理数的连分数展开

本节中讨论实二次无理数的三种连分数展开式，即简单连分数、半单连分数和奇异连分数。前两者在实二次域类数问题的研究中起着非常重要的作用，后者则在研究实二次欧氏域时起着关键的作用。

1.1 简单连分数

对一个实数 α，可如下地定义 α 的简单连分数展开式(见华罗庚著《数论导引》第十章，这里为了引用的方便，给出概况)：

令 $\alpha_0=\alpha$，对 $n\geqslant 0$，归纳地定义

$a_n=[\alpha_n]$，$\alpha_{n+1}=(\alpha_n-a_n)^{-1}$，如 $a_n\neq\alpha_n$，$a_n\in\mathbb{Z}$ $(n\geqslant 0)$，$a_n\geqslant 1(n\geqslant 1)$。 (1.1)

其中 $[x]$ 表 x 的整数部分。

我们记

$$\alpha=[a_0,\ a_1,\ \cdots,\ a_n,\ \cdots], \tag{1.2}$$

α_n称为α的第n个完全商。

$$\frac{p_n}{q_n}=[a_0, a_1, \cdots, a_n](n\geqslant 0) \tag{1.3}$$

称为α的第n个渐近分数，其中要求p_n、q_n为互素的整数，且$q_n\geqslant 1(n\geqslant 0)$。熟知有

$$p_nq_{n-1}-p_{n-1}q_n=(-1)^{n-1}(n\geqslant 1), \tag{1.4}$$

$$p_0=a_0,\ p_1=a_0a_1+1,\ p_n=a_np_{n-1}+p_{n-2}(n\geqslant 2), \tag{1.5}$$

$$q_0=1,\ q_1=a_1,\ q_n=a_nq_{n-1}+q_{n-2}(n\geqslant 2), \tag{1.6}$$

$$\alpha_n=[a_n, a_{n+1}, \cdots](n\geqslant 0). \tag{1.7}$$

有时还约定

$$p_{-1}=1,\ q_{-1}=0. \tag{1.8}$$

这样$n=0$时，(1.4)式仍成立。

设a, b, c为有理整数，它们满足

$$0\leqslant |b|\leqslant a\leqslant c, \tag{1.9}$$

且$d=b^2+4ac$不是完全平方。易见

$$1\leqslant a<\frac{\sqrt{d}}{2}. \tag{1.10}$$

实二次无理数

$$\alpha=\frac{b+\sqrt{d}}{2a}>0 \tag{1.11}$$

满足二次方程

$$ax^2-bx-c=0, \tag{1.12}$$

这个方程的另一个根是

$$\alpha'=\frac{b-\sqrt{d}}{2a}. \tag{1.13}$$

α'也是α在Galois群$\mathrm{Gal}(Q(\sqrt{d})/Q)$下的象。

命α的简单连分数展开式为

$$\alpha=[a_0, a_1, \cdots, a_n, \cdots],\ a_n\in\mathbb{Z},\ a_0\geqslant 0,\ a_n\geqslant 1(n\geqslant 1), \tag{1.14}$$

并用(1.1)—(1.13)的记号。再命

$$Q_0=a,\ P_0=b,\ P_1=2a_0a-b, \tag{1.15}$$

$$Q_n=(-1)^n(ap_{n-1}^2-bp_{n-1}q_{n-1}-cq_{n-1}^2)\ (n\geqslant 0),\quad (1.16)$$

$$P_n=(-1)^{n-1}(2ap_{n-1}p_{n-2}-b(p_{n-1}q_{n-2}+p_{n-2}q_{n-1})-2cq_{n-1}q_{n-2})\ (n\geqslant 1).\quad (1.17)$$

易见诸 Q_n、$P_n(n\geqslant 0)$ 均为有理整数．且有

引理 1.1
$$P_n^2+4Q_nQ_{n-1}=d\ (n\geqslant 1),\quad (1.18)$$

$$P_{n+1}+P_n=2a_nQ_n\ (n\geqslant 0),\quad (1.19)$$

$$Q_{n+1}=Q_{n-1}+a_nP_n-a_n^2Q_n\ (n\geqslant 1),\quad (1.20)$$

$$1\leqslant Q_n<\sqrt{d}\ (n\geqslant 0),\quad (1.21)$$

$$P_n\geqslant 1\quad (n\geqslant 1),\quad (1.22)$$

$$P_n<\sqrt{d}\ (n\geqslant 0).\quad (1.23)$$

证明 (1.18)与(1.19)由直接计算可得．(1.20)是(1.18)与(1.19)的推论．又由定义(1.16)可得

$$Q_n=(-1)^n aq_{n-1}^2\left(\frac{p_{n-1}}{q_{n-1}}-\alpha\right)\left(\frac{p_{n-1}}{q_{n-1}}-\alpha'\right)(n\geqslant 1),\quad (1.24)$$

由(1.9)与(1.10)即有 $\alpha'<0$, 再由(1.4)可得

$$(-1)^n\left(\frac{p_{n-1}}{q_{n-1}}-\alpha\right)>0\ (n\geqslant 1).\quad (1.25)$$

这样由(1.24)即得 $Q_n>0(n\geqslant 1)$, 从而 $Q_n\geqslant 1(n\geqslant 0)$, 这证明了(1.21)的前一半．

如 $a_0\geqslant 1$, 则 $P_1=2a_0a-b\geqslant 2a-b\geqslant a\geqslant 1$; 如 $a_0=0$, 则 $\alpha<1$, 故由 (1.10) 即有 $b<0$, 从而仍有 $P_1=-b\geqslant 1$. 总之有 $P_1\geqslant 1$. 当 $n\geqslant 2$ 时, 由定义(1.17)有

$$P_n=(-1)^{n-1}q_{n-1}q_{n-2}\left(2a\frac{p_{n-1}}{q_{n-1}}\cdot\frac{p_{n-2}}{q_{n-2}}-b\left(\frac{p_{n-1}}{q_{n-1}}+\frac{p_{n-2}}{q_{n-2}}\right)-2c\right)\quad (1.26)$$

易见有

$$\alpha=\frac{\alpha_np_{n-1}+p_{n-2}}{\alpha_nq_{n-1}+q_{n-2}}\ (n\geqslant 2).\quad (1.27)$$

由(1.26)、(1.27)有

$$P_n=(-1)^{n-1}q_{n-1}q_{n-2}\left(2a\left(\alpha+\frac{(-1)^n}{q_{n-1}(q_{n-1}\alpha_n+q_{n-2})}\right)\right.$$

$$\cdot\left(\alpha+\frac{(-1)^{n-1}\alpha_n}{q_{n-2}(q_{n-1}\alpha_n+q_{n-2})}\right)$$
$$-b\left(2\alpha+\frac{(-1)^n}{q_{n-1}(q_{n-1}\alpha_n+q_{n-2})}+\frac{(-1)^{n-1}\alpha_n}{q_{n-2}(q_{n-1}\alpha_n+q_{n-2})}\right)-2c\Bigg)$$
$$=q_{n-1}q_{n-2}\left((2a\alpha-b)\frac{q_{n-1}\alpha_n-q_{n-2}}{q_{n-1}q_{n-2}(q_{n-1}\alpha_n+q_{n-2})}\right.$$
$$\left.+\frac{2a(-1)^n\alpha_n}{q_{n-1}q_{n-2}(q_{n-1}\alpha_n+q_{n-2})^2}\right),$$

其中用到α是方程(1.12)的一个根，从而得到

$$P_n=\frac{\sqrt{d}\,(q_{n-1}^2\alpha_n^2-q_{n-2}^2)+(-1)^n2a\alpha_n}{(q_{n-1}\alpha_n+q_{n-2})^2}\quad(n\geqslant 2)。\qquad(1.28)$$

$n=2$时，(1.28)右边分子的两项均非负，而第二项为正，故$P_2\geqslant 1$。而$n\geqslant 3$时，由于

$$q_{n-1}^2\alpha_n-q_{n-2}^2\alpha_n^{-1}>q_{n-1}^2-q_{n-2}^2\geqslant 2,$$

故(1.28)右边的分子

$$=\alpha_n(\sqrt{d}\,(q_{n-1}^2\alpha_n-q_{n-2}^2\alpha_n^{-1})+(-1)^n2a)$$
$$>\alpha_n(2\sqrt{d}-2a)>0。$$

从而$n\geqslant 3$时，也有$P_n\geqslant 1$。引理的其余部分显然成立。引理证毕。

引理 1.2 我们有

$$\alpha_n=\frac{P_n+\sqrt{d}}{2Q_n}\quad(n\geqslant 0);\qquad(1.29)$$

$$\sqrt{d}-P_n<2Q_n<\sqrt{d}+P_n(n\geqslant 1);\qquad(1.30)$$

$$\sqrt{d}-P_{n+1}<2Q_n<\sqrt{d}+P_{n+1}(n\geqslant 0);\qquad(1.31)$$

$$a_n=\left[\frac{P_n+\sqrt{d}}{2Q_n}\right]\quad(n\geqslant 0);\qquad(1.32)$$

$$a_n=\left[\frac{2Q_{n+1}}{\sqrt{d}-P_{n+1}}\right](n\geqslant 1)。\qquad(1.33)$$

证明 (1.29)由定义、引理1.1及归纳法可得。(1.30)的右端显然成立，至于左端用引理1.1即有

$$\frac{2Q_n}{\sqrt{d}-P_n}=\frac{\sqrt{d}+P_n}{2Q_{n-1}}>\frac{P_{n-1}+P_n}{2Q_{n-1}}=a_{n-1}\geqslant 1,$$

如$n\geqslant 2$或$n=1$而$a_0\geqslant 1$。但当$n=1$而$a_0=0$时，由引理1.1的

证明可知 $b<0$，从而有 $Q_1=c$，$P_1=-b=|b|$，所以由(1.9)及 a_0 的定义即有

$$2Q_1=2c\geqslant 2a>b+\sqrt{d}=\sqrt{d}-P_1.$$

这就证明了(1.30)。

(1.32)是(1.29)的推论，于是有（注意由(1.23)知 $\sqrt{d}>P_{n+1}$）

$$\frac{2Q_n}{\sqrt{d}-P_{n+1}}>\left[\frac{2Q_n}{\sqrt{d}-P_{n+1}}\right]=\left[\frac{P_{n+1}+\sqrt{d}}{2Q_{n+1}}\right]=a_{n+1}\geqslant 1\ (n\geqslant 0),$$

由此即得(1.31)的左端。至于右端用引理1.1即有

$$\frac{\sqrt{d}+P_{n+1}}{2Q_n}>\frac{P_n+P_{n+1}}{2Q_n}=a_n\geqslant 1,\quad \text{如 } n\geqslant 1 \text{ 或 } n=0 \text{ 而 } a_0\geqslant 1$$

时；但当 $n=0$ 且 $a_0=0$ 时，有

$$\frac{\sqrt{d}+P_1}{2Q_0}=\frac{\sqrt{d}+|b|}{2a}>1,$$

所以(1.31)完全得证。由(1.30)、(1.19)、(1.18)可得

$$a_n=\left[a_n+\frac{\sqrt{d}-P_n}{2Q_n}\right]=\left[\frac{\sqrt{d}+P_{n+1}}{2Q_n}\right]$$

$$=\left[\frac{2Q_{n+1}}{\sqrt{d}-P_{n+1}}\right](n\geqslant 1).$$

即得(1.33)。引理证毕。

由引理1.2即知 α 的简单连分数展开式为：

$$\alpha=[a_0,\ \overline{a_1,\ \cdots,a_k}]. \tag{1.34}$$

这个记号意指

$$a_{k+n}=a_n\quad(n\geqslant 1). \tag{1.35}$$

我们取 k 为最小可能的，$\overline{a_1,\ \cdots,a_k}$ 称为基本周期，k 称为周期的长度。

这样可有

$$P_{k+1}=P_1,\ Q_{k+1}=Q_1,\ a_{k+1}=a_1, \tag{1.36}$$

$$Q_k=\frac{d-P_{k+1}^2}{4Q_{k+1}}=\frac{d-P_1^2}{4Q_1}=Q_0=a, \tag{1.37}$$

$$a_k=\left[\frac{2Q_{k+1}}{\sqrt{d}-P_{k+1}}\right]=\left[\frac{\sqrt{d}+P_{k+1}}{2Q_k}\right]=\left[\frac{\sqrt{d}+P_1}{2Q_0}\right]$$

$$=\left[\frac{\sqrt{d}+2a_0a-b}{2a}\right]=2a_0+\left[\frac{\sqrt{d}-2a_0a-b}{2a}\right]$$

$$=2a_0+\left[\frac{\sqrt{d}-P_1}{2Q_0}-\frac{b}{a}\right]$$

$$=\begin{cases}2a_0 \text{ 或 } 2a_0-1, & \text{当 } b\geqslant 0;\\ 2a_0 \text{ 或 } 2a_0+1, & \text{当 } b<0.\end{cases} \tag{1.38}$$

引理 1.3 当 $b=0$ 或 $\pm a$ 时，有

$$a_n=a_{k-n}(1\leqslant n\leqslant k-1), \tag{1.39}$$

$$Q_n=Q_{k-n}(1\leqslant n\leqslant k-1), \tag{1.40}$$

$$P_n=P_{k+1-n}(1\leqslant n\leqslant k-1), \tag{1.41}$$

$$a_k=\begin{cases}2a_0, & \text{当 } b=0 \text{ 时};\\ 2a_0-1, & \text{当 } b=a \text{ 时};\\ 2a_0+1, & \text{当 } b=-a \text{ 时}.\end{cases} \tag{1.42}$$

并且有

(1) 如 $P_l=P_{l+1}$ 对某个满足 $1\leqslant l<l+1\leqslant k$ 的 l 成立，则有 $k=2l$；

(2) 如 $Q_{l-1}=Q_{l+1}$ 对某个满足 $1\leqslant l-1<l+1\leqslant k-1$ 的 l 成立，则有 $k=2l$；

(3) 如 $Q_l=Q_{l+1}$ 对某个满足 $1\leqslant l<l+1\leqslant k-1$ 的 l 成立，则有 $k=2l+1$。

证明 由 (1.38) 及其之前的计算，即得(1.42)。又有 $Q_k=Q_0$, $P_{k+1}=P_1$, 故由

$$P_k=2a_kQ_k-P_{k+1}=2a_kQ_0-P_1,$$

结合(1.42)分别计算之，即得

$$P_k=P_1.$$

于是

$$Q_{k-1}=\frac{d-P_k^2}{4Q_k}=\frac{d-P_1^2}{4Q_0}=Q_1,$$

$$a_{k-1}=\left[\frac{2Q_k}{\sqrt{d}-P_k}\right]=\left[\frac{2Q_0}{\sqrt{d}-P_1}\right]=\left[\frac{\sqrt{d}+P_1}{2Q_1}\right]=a_1,$$

$$P_{k-1}=2a_{k-1}Q_{k-1}-P_k=2a_1Q_1-P_1=P_2,$$

如此继续做下去，即得(1.39)—(1.41)。

最后三个断言也容易证明。引理证毕。

附记　这个引理可使在计算 $\alpha=\frac{b+\sqrt{d}}{2a}$ 的简单连分数展开式时减少工作量，如果 $a|b$ 这一条件成立的话。

引理 1.4　如 $b=0$, $a=1$ 或 $b=a=1$，则有

$$Q_n\geqslant 2(1\leqslant n\leqslant k-1),\ Q_k=Q_0=1, \tag{1.43}$$

$$1\leqslant a_n\leqslant a_0(1\leqslant n\leqslant k-1). \tag{1.44}$$

证明　$Q_k=Q_0=1$，即(1.43)的后一式显然成立。如有 n 满足 $1\leqslant n\leqslant k-1$，使 $Q_n=1$。则

$$\alpha_n=\frac{P_n+\sqrt{d}}{2}=\frac{P_n-b}{2}+\alpha,$$

又由(1.18)知 P_n 与 b 同奇偶。这样，得出

$$\alpha=[a_0,\ a_1,\ \cdots,\ a_{n-1},\ \alpha_n]=\left[a_0,\ \overline{a_1,\ \cdots,\ a_{n-1},\ \frac{P_n-b}{2}+a_0}\right],$$

这与 k 的定义矛盾。这样完全证明了(1.43)。

(1.44)的左端是显然的，至于右端，由(1.43)即知，对 $1\leqslant n\leqslant k-1$ 有

$$a_n=\frac{P_n+P_{n+1}}{2Q_n}\leqslant\frac{2[\sqrt{d}]}{4}=\frac{[\sqrt{d}]}{2},$$

故

$$a_n\leqslant\left[\frac{[\sqrt{d}]}{2}\right]\leqslant\left[\frac{b+[\sqrt{d}]}{2}\right]\leqslant\left[\frac{b+\sqrt{d}}{2}\right]=a_0.$$

引理证毕。

引理 1.5　设 a、b、c、d 仍如上所述，而且 $\alpha=\frac{b+\sqrt{d}}{2a}$ 的简单连分数展开式为

$$\alpha=[a_0,\ \overline{a_1,\ a_2,\ \cdots,\ a_{k-1},\ a_k}],$$

其中 $\overline{a_1,\ a_2,\ \cdots,\ a_{k-1},\ a_k}$ 为基本周期。

再令 α 的第 n 个完全商为

$$\alpha_n=[a_n,\ a_{n+1},\ \cdots]=\frac{P_n+\sqrt{d}}{2Q_n}\quad(n\geqslant 0).$$

则 $\beta=-\alpha'=\frac{-b+\sqrt{d}}{2a}$ 的简单连分数展开式为

$$\beta=[a_k-a_0,\ \overline{a_{k-1},\ a_{k-2},\ \cdots,\ a_2,\ a_1,\ a_k}].$$

其中 $\overline{a_{k-1},\ a_{k-2},\ \cdots,\ a_1,\ a_k}$ 为基本周期。而且 β 的第 n 个完全商

$$\beta_n=\frac{P_{k+1-n}+\sqrt{d}}{2Q_{k-n}}\quad(1\leqslant n\leqslant k).$$

证明 不妨设 $b\geqslant0$（否则可对调 α 与 β）。这样有 $a_0\geqslant1$，$a_k\geqslant2a_0-1\geqslant a_0$，即有 $a_k-a_0\geqslant0$。用引理 1.1 以及引理 1.3 之前的计算，我们有

$$\begin{aligned}
\beta&=\frac{-b+\sqrt{d}}{2a}=a_k-a_0+\frac{\sqrt{d}-b-2a(a_k-a_0)}{2a}\\
&=a_k-a_0+\frac{\sqrt{d}+P_1-2a_ka}{2a}\\
&=a_k-a_0+\frac{\sqrt{d}+P_{k+1}-2a_kQ_k}{2Q_k}\\
&=a_k-a_0+\frac{\sqrt{d}-P_k}{2Q_k}\\
&=\left[a_k-a_0,\ \frac{2Q_k}{\sqrt{d}-P_k}\right]=\left[a_k-a_0,\ \frac{\sqrt{d}+P_k}{2Q_{k-1}}\right]\\
&=\left[a_k-a_0,\ a_{k-1}+\frac{\sqrt{d}-P_{k-1}}{2Q_{k-1}}\right]\\
&=\left[a_k-a_0,\ a_{k-1},\ \frac{2Q_{k-1}}{\sqrt{d}-P_{k-1}}\right]\\
&=\cdots\cdots\\
&=\left[a_k-a_0,\ a_{k-1},\ a_{k-2},\ \cdots,\ a_{n+1},\ a_n,\ \frac{2Q_n}{\sqrt{d}-P_n}\right]\\
&\quad(1\leqslant n\leqslant k-1)\\
&=\cdots\cdots\\
&=\left[a_k-a_0,\ a_{k-1},\ a_{k-2},\ \cdots,\ a_2,\ a_1,\ \frac{2Q_1}{\sqrt{d}-P_1}\right]\\
&=\left[a_k-a_0,\ a_{k-1},\ a_{k-2},\ \cdots,\ a_2,\ a_1,\ \frac{\sqrt{d}+P_1}{2Q_0}\right]\\
&=\left[a_k-a_0,\ a_{k-1},\ a_{k-2},\ \cdots,\ a_2,\ a_1,\ a_0+\frac{\sqrt{d}-b}{2a}\right],
\end{aligned}$$

即有
$$\beta=[a_k-a_0,\ a_{k-1},\ a_{k-2},\ \cdots,\ a_2,\ a_1,\ a_0+\beta]$$
$$=[a_k-a_0,\ \overline{a_{k-1},\ a_{k-2},\ \cdots,\ a_2,\ a_1,\ a_k}].$$
引理证毕。

附记 由引理1.5知引理1.4在 $b=-a=-1$ 时，仍成立。

引理 1.6 设 r、s 为互素的正整数，实数 α,β 满足 $0<\beta\leqslant\alpha$。如有
$$|(r-\alpha s)(r+\beta s)|<\frac{\alpha+\beta}{2},$$
则 $\frac{r}{s}$ 是 α 的简单连分数展开式的一个渐近分数。

证明 这是华罗庚著《数论导引》p.283定理3的推广，那里讨论了 $\alpha=\beta$ 的情况。仿照那里的办法，令
$$(s\alpha-r)(s\beta+r)=\varepsilon\delta\frac{\alpha+\beta}{2},\ \varepsilon=\pm1,\ 0\leqslant\delta<1,$$
并展开 $\frac{r}{s}$ 为有限的简单连分数
$$\frac{r}{s}=[b_0,\ b_1,\ \cdots,\ b_{l-1}],\ (-1)^{l-1}=\varepsilon.$$

由
$$s\alpha-r=\frac{\varepsilon\delta\frac{\alpha+\beta}{2}}{s\beta+r}$$
可得
$$\theta\overset{\text{def}}{=\!=}\varepsilon s(s\alpha-r)=\frac{\delta\frac{\alpha+\beta}{2}s}{s\beta+r}\geqslant0.$$

首先可以断定 $\theta<1$。为此只需证明
$$\frac{\alpha+\beta}{2}s\leqslant s\beta+r. \tag{1.45}$$
如果此式不成立，则有
$$\alpha s-r>s\beta+r \text{ 与 } \frac{\alpha+\beta}{2}<\alpha-\frac{r}{s},$$
以此代入引理中的不等式，即得
$$s(s\beta+r)<1,$$
此不可能，因为 $\beta>0$ 且 r、s 是正整数。这证明了

$$0 \leqslant \theta < 1.$$

如$\theta=0$，则有$\frac{r}{s}=\alpha$，$\frac{r}{s}$当然是α的一个渐近分数。因此可设

$$0 < \theta < 1.$$

命$\frac{r}{s}$的渐近分数为

$$\frac{p_i'}{q_i'} (0 \leqslant i \leqslant l-1),$$

则$r=p_{l-1}'$，$s=q_{l-1}'$，从而有

$$\theta = \frac{\delta \frac{\alpha+\beta}{2} q_{l-1}'}{q_{l-1}'\beta + p_{l-1}'}.$$

由上述所引华罗庚著《数论导引》p.283的定理1可知，为了证明我们的引理，只需证明

$$\frac{\delta \frac{\alpha+\beta}{2} q_{l-1}'}{q_{l-1}'\beta + p_{l-1}'} \leqslant \frac{q_{l-1}'}{q_{l-1}' + q_{l-2}'},$$

即只需证明

$$\delta \frac{\alpha+\beta}{2} (q_{l-1}' + q_{l-2}') \leqslant q_{l-1}'\beta + p_{l-1}'.$$

当$l=1$时，$s=1$，此时只需证明

$$\frac{\alpha+\beta}{2} \leqslant \beta + r,$$

由已证明的(1.45)，这是成立的。

当$l=2$时，$q_0'=1$，$q_1'=s$，$p_1'=r$。此时只需证明

$$\frac{\alpha+\beta}{2}(s+1) \leqslant s\beta + r.$$

由于这时有$\varepsilon=-1$，故有$r-s\alpha>0$，即有$\alpha<\frac{r}{s}$，从而有

$$\begin{aligned}\frac{\alpha+\beta}{2}(s+1) - s\beta - r &< \frac{s+1}{2}\left(\frac{r}{s}+\beta\right) - s\beta - r \\ &= \frac{1-s}{2}\left(\beta + \frac{r}{s}\right) \leqslant 0,\end{aligned}$$

得到所需要的不等式。

最后，当 $l\geqslant 3$ 时，只需证明

$$\frac{\alpha+\beta}{2}(q'_{l-1}+q'_{l-2})\leqslant q'_{l-1}\beta+p'_{l-1},$$

即
$$\alpha q'_{l-1}-p'_{l-1}\leqslant\frac{\alpha+\beta}{2}(q'_{l-1}-q'_{l-2}),$$

也即

$$\frac{\varepsilon\delta\,\frac{\alpha+\beta}{2}}{q'_{l-1}\beta+p'_{l-1}}\leqslant\frac{\alpha+\beta}{2}(q'_{l-1}-q'_{l-2}).$$

这在 $l\geqslant 3$ 时，显然成立。引理证毕。

引理 1.7　设有理整数 a、b、c 满足 $0\leqslant b\leqslant a\leqslant c$，且 $d=b^2+4ac$ 不是一个完全平方，从而 $a\geqslant 1$。再设互素的正整数 r、s 满足不等式

$$|ar^2-brs-cs^2|<\frac{\sqrt{d}}{2},$$

则 $\frac{r}{s}$ 是 $\alpha=\frac{b+\sqrt{d}}{2a}$ 的简单连分数展开式的一个渐近分数。

证明　令

$$\beta=-\alpha'=\frac{-b+\sqrt{d}}{2a},$$

则有

$$|(r-\alpha s)(r+\beta s)|<\frac{\sqrt{d}}{2a}=\frac{\alpha+\beta}{2},$$

且有 $0<\beta\leqslant\alpha$。因此由引理 1.6 即得所需。引理获证。

1.2　半单连分数

一个实数 $\omega>1$，可以如下地展开为半单连分数：

令 $\omega_0=\omega$，对 $n\geqslant 0$ 归纳地定义

$$b_n=1+[\omega_n],\ \omega_{n+1}=(b_n-\omega_n)^{-1},$$

记为
$$\omega=[[b_0,\ b_1,\ b_2,\ \cdots,\ b_n,\ \cdots]]$$

引理 1.8　设无理数 $\omega>1$ 的简单连分数展开式为

$$\omega=[a_0,\ a_1,\ \cdots,\ a_n,\ \cdots],$$

则ω的半单连分数展开式为：

$$\omega=[[a_0+1,\ \underbrace{2,\ \cdots,\ 2}_{a_1-1\text{个}},\ a_2+2,\ \underbrace{2,\ \cdots,\ 2}_{a_3-1\text{个}},\ a_4+2,\ \cdots,\ \underbrace{2,\ \cdots,\ 2}_{a_{2n-1}-1\text{个}},\ a_{2n}+2,\ \cdots]].$$

证明 首先用归纳法容易证明

$$[[\underbrace{2,\ 2,\ \cdots,\ 2}_{n\text{个}},\ \beta]]=\frac{(n+1)\beta-n}{n\beta-(n-1)}. \tag{1.46}$$

现设

$$\omega=[[b_0,\ b_1,\ \cdots,\ b_n,\ \cdots]].$$

第一步易见有

$$b_0=a_0+1. \tag{1.47}$$

如$b_1\geqslant 3$，则由

$$[a_0,\ a_1,\ a_2,\ \cdots]=\omega=[[b_0,\ b_1,\ b_2,\ \cdots]],$$

可得

$$[a_1,\ a_2,\ \cdots]=\frac{1}{[[1,\ b_1,\ b_2,\ \cdots]]}<\frac{1}{1-\frac{1}{2}}=2,$$

于是

$$a_1=1,\ \text{如}\ b_1\geqslant 3. \tag{1.48}$$

设$b_1=b_2=\cdots=b_n=2$，而$b_{n+1}\geqslant 3$，则由

$$\begin{aligned}[a_0,\ a_1,\ a_2,\ \cdots]&=\omega=[[b_0,\ b_1,\ b_2,\ \cdots,\ b_n,\ \cdots]]\\&=[[a_0+1,\ \underbrace{2,\ 2,\ \cdots,\ 2}_{n\text{个}},\ b_{n+1},\ \cdots]]\end{aligned}$$

及(1.46)可得

$$\begin{aligned}[a_1,\ a_2,\ \cdots]&=\cfrac{1}{1-\cfrac{1}{[[\underbrace{2,\ 2,\ \cdots,\ 2}_{n\text{个}},\ b_{n+1},\ \cdots,]]}}\\&=\frac{1}{1-\frac{nr-(n-1)}{(n+1)r-n}}=n+1+\frac{1}{r-1},\end{aligned}$$

其中$r=[[b_{n+1},\ \cdots]]>2$。于是

$$a_1=n+1, \text{ 如 } b_1=b_2=\cdots=b_n=2, \text{ 而 } b_{n+1}\geqslant 3. \quad (1.49)$$

由(1.48)与(1.49)即有

$b_1=b_2=\cdots=b_{a_1-1}=2$, 但 $b_{a_1}\geqslant 3$, 以及

$$[a_2, a_3, \cdots]=[[b_{a_1}, b_{a_1+1}, \cdots]]-1$$
$$=b_{a_1}-1-\frac{1}{[[b_{a_1+1}, \cdots]]},$$

从而有(并用(1.47))

$$b_{a_1}-1=a_2+1, \text{ 即 } b_{a_1}=a_2+2.$$

如此继续做下去，即得引理。

定义 1.1 两个实数 ω 与 β 称为相似的，并记为 $\omega\sim\beta$, 如果存在有理整数 u、v、r、s 使有

$$us-vr=\pm 1, \text{ 且 } \omega=\frac{u\beta+v}{r\beta+s};$$

当 $us-vr=1$ 时，ω 与 β 称为严格相似的，记为 $\omega\approx\beta$。

由华罗庚著《数论导引》p.277 定理 3 即知，两个实的无理数 ω 与 β 相似的充要条件是

$$\omega=[a_0, a_1, \cdots, a_m, c_0, c_1, \cdots],$$
$$\beta=[b_0, b_1, \cdots, b_n, c_0, c_1, \cdots].$$

也即它们的简单连分数展开式自有限项以后完全相同，并且相似方阵 $\begin{pmatrix} u & v \\ r & s \end{pmatrix}$ 的行列式 $us-vr=(-1)^{m+n}$。

定义 1.2 一个实二次无理数 ω 称为约化的，如其满足

$$0<\omega'<1<\omega,$$

其中 ω' 是 ω 所满足的二次有理系数方程的另一个根。

引理 1.9 设有理整数 a、b、c 满足 $0\leqslant|b|\leqslant a\leqslant c$, 且 $d=b^2+4ac$ 不是一个完全平方。命

$$\mathfrak{M}=\left\{\omega=\frac{P+\sqrt{d}}{2Q}\;\middle|\;\begin{array}{l}P, Q\in\mathbb{Z}, Q\neq 0, P\equiv d(\bmod 2), \\ Q\mid\frac{P^2-d}{4}, \omega \text{ 约化}\end{array}\right\}.$$

设 $\alpha=\dfrac{b+\sqrt{d}}{2a}$ 的简单连分数展开式为

$$\alpha=[a_0,\overline{a_1,\ \cdots,\ a_k}],$$

其中$\overline{a_1,\ \cdots,\ a_k}$为基本周期，并且$\alpha$的第$n$个完全商为

$$\alpha_n=\frac{P_n+\sqrt{d}}{2Q_n}\ (n\geqslant 0).$$

再命

$$\mathfrak{M}_x=\left\{\omega\in\mathfrak{M}\ \middle|\ \omega\sim\beta=-\alpha'=\frac{-b+\sqrt{d}}{2a}\right\},$$

则我们有下列的结论：

(1) $|\mathfrak{M}|=\dfrac{1}{2}\sum\limits_{\substack{|m|<\sqrt{d}\\ m\equiv d(\operatorname{mod}2)}}\tau\left(\dfrac{d-m^2}{4}\right)$,

这里$\tau(*)$表示除数函数，即$\tau(x)$是x的正因子的个数；

(2) $|\mathfrak{M}_x|=\sum\limits_{n=1}^{k}a_n$;

(3) $\mathfrak{M}_x=\left\{\dfrac{P+\sqrt{d}}{2Q}\ \middle|\ \begin{array}{l}P=2Q_{n+1}-P_{n+1}+2(P_{n+1}+Q_n)t\\ \quad -2Q_nt^2,\\ Q=Q_{n+1}+tP_{n+1}-t^2Q_n,\\ 1\leqslant t\leqslant a_n,\ 1\leqslant n\leqslant k.\end{array}\right\}$.

证明　首先来证明下列的断言.

断言　$\omega=\dfrac{P+\sqrt{d}}{2Q}\in\mathfrak{M}$的充要条件是$\omega$的半单连分数展开式是纯循环的，即

$$\omega=[[\overline{b_0,\ b_1,\ \cdots,\ b_m}]],$$

其中$\overline{b_0,b_1,\cdots,\ b_m}$为基本周期.

必要性：命$\omega_n=[[b_n,\ b_{n+1},\ \cdots]]\ (n\geqslant 0)$, $\omega_0=\omega=\dfrac{P+\sqrt{d}}{2Q}$.
用归纳法即知由ω_0的约化可以推出$\omega_n(n\geqslant 0)$均是约化的，即有

$$0<\omega_n'<1<\omega_n\ (n\geqslant 0).$$

(注意，我们有$b_n\geqslant 2\ (n\geqslant 0)$).

命$P_0'=P$, $Q_0'=Q$. 则有

$$\omega_0=b_0-\frac{1}{\omega_1},\ \ \omega_1=\frac{1}{b_0-\omega_0}=\frac{2Q_0'}{P_1'-\sqrt{d}},$$
$$P_1'=2b_0Q_0'-P_0'\in\mathbb{Z},$$

又 $P_1'^2 - d = (2b_0Q_0' - P_0')^2 - d = 4Q_0'Q_1'$，其中 $Q_1' = b_0^2Q_0' - b_0P_0' + \dfrac{P_0'^2 - d}{4Q_0'} \in \mathbb{Z}$。

从而有

$$\omega_n = \frac{P_n' + \sqrt{d}}{2Q_n'},\ P_n'、Q_n' \in \mathbb{Z}\,(n = 0, 1),$$

$$P_1' + P_0' = 2b_0Q_0',\ P_1'^2 - 4Q_0'Q_1' = d.$$

由 $0 < \omega_n' = \dfrac{P_n' - \sqrt{d}}{2Q_n'} < 1 < \omega_n = \dfrac{P_n' + \sqrt{d}}{2Q_n'}\ (n = 0,\ 1)$，

即知有

$$Q_n' > 0, \max\{\sqrt{d},\ 2Q_n' - \sqrt{d}\} < P_n' < 2Q_n' + \sqrt{d}\ (n = 0, 1).$$

如此继续下去，可得

$$\omega_n = \frac{P_n' + \sqrt{d}}{2Q_n'},\ P_n',\ Q_n' \in \mathbb{N}\,(n \geqslant 0),$$

$$P_{n+1}' + P_n' = 2b_nQ_n'\,(n \geqslant 0),$$

$$P_{n+1}'^2 - 4Q_n'Q_{n+1}' = d\,(n \geqslant 0),$$

$$\max\{\sqrt{d},\ 2Q_n' - \sqrt{d}\} < P_n' < 2Q_n' + \sqrt{d}\ (n \geqslant 0).$$

这样，对 $n \geqslant 0$，我们有

$$b_n - 1 = b_n + [-\omega_n'] = \left[b_n + \frac{\sqrt{d} - P_n'}{2Q_n'}\right]$$

$$= \left[\frac{P_{n+1}' + \sqrt{d}}{2Q_n'}\right] = \left[\frac{Q_{n+1}'}{P_{n+1}' - \sqrt{d}}\right],$$

从而得到

$$b_n = \left[\frac{2Q_{n+1}'}{P_{n+1}' - \sqrt{d}}\right] + 1\ \ (n \geqslant 0).$$

由此即知 ω 的半单连分数展开式是纯循环的。

充分性：此时有 $\omega > 1$ 和

$$\omega = [[b_0,\ b_1,\ \cdots,\ b_m,\ \omega]].$$

我们指出 $b_n \geqslant 2\,(n \geqslant 0)$。再命

$$\frac{p_n'}{q_n'} = [[b_0,\ b_1,\ \cdots,\ b_n]]\ (n \geqslant 0).$$

则用归纳法可得

$$p_n',\ q_n' \in \mathbb{N},\ g.c.d.(p_n',\ q_n') = 1\quad (n \geqslant 0),$$

$$p_0'=b_0,\ p_1'=b_0b_1-1,\ p_n'=b_np_{n-1}'-p_{n-2}'(n\geqslant 2),$$
$$p_n'>p_{n-1}'(n\geqslant 1).$$
$$q_0'=1,\ q_1'=b_1,\ q_n'=b_nq_{n-1}'-q_{n-2}'(n\geqslant 2),\ q_n'>q_{n-1}'(n\geqslant 1),$$
$$p_{n-1}'q_n'-p_n'q_{n-1}'=1\quad(n\geqslant 1).$$

由此即知

$$\omega'=[[b_0,\ b_1,\ \cdots,\ b_m,\ \omega']]=\frac{u\omega'-v}{r\omega'-s},$$

其中 u、v、r 为正整数，而 s 为非负整数。这样

$$r\omega'=u+s-\frac{v}{\omega'},$$

由该式即知有 $\omega'>0$。因为如有 $\omega'<0$，则有 $r\omega'>0$，得出矛盾。

我们再证明 $\omega'<1$。如有 $\omega'>1$，则 ω' 有半单连分数展开式，这样得到

$$\omega'=[[b_0,\ b_1,\ \cdots,\ b_m,\ \omega']]=[[\overline{b_0,\ b_1,\ \cdots,\ b_m}]]=\omega,$$

这不可能。这样我们证明了 $0<\omega'<1<\omega$，即 ω 是约化。总之完成了断言的证明。

现在我们由这一断言来证明引理。

先证明(1)：容易看出有

$$|\mathfrak{M}|=\sum_{\substack{0<\frac{P-\sqrt{d}}{2Q}<1<\frac{P+\sqrt{d}}{2Q}\\ P\equiv d\,(\mathrm{mod}\,2),\ Q\neq 0\\ Q\mid\frac{P^2-d}{4}}}1=\sum_{\substack{|P-2Q|<\sqrt{d}<P\\ Q>0,\ P\equiv d\,(\mathrm{mod}\,2)\\ Q\mid\frac{P^2-d}{4}}}1,$$

命 $m=P-2Q$，即得

$$|\mathfrak{M}|=\sum_{\substack{|m|<\sqrt{d},\ m\equiv d\,(\mathrm{mod}\,2)\\ 1\leqslant Q\mid\frac{d-m^2}{4},\ \frac{\sqrt{d}-m}{2Q}<1}}1=\sum_{1\leqslant Q\mid\frac{d}{4},\ \frac{d}{2Q}<1}1+\sum_{\substack{1\leqslant m<\sqrt{d},\ m\equiv d\,(\mathrm{mod}\,2)\\ 1\leqslant Q\mid\frac{d-m^2}{4},\ \frac{\sqrt{d}-m}{2Q}<1}}1+\sum_{\substack{1\leqslant m<\sqrt{d},\ m\equiv d\,(\mathrm{mod}\,2)\\ 1\leqslant Q\mid\frac{d-m^2}{4},\ \frac{\sqrt{d}+m}{2Q}<1}}1,$$

以上第一个和，当 $4\nmid d$ 时是 0；当 $4\mid d$ 时，为

$$\sum_{1\leqslant Q\mid\frac{d}{4},\ \frac{\sqrt{d}}{2Q}<1} 1=\sum_{1\leqslant Q\mid\frac{d}{4},\ \frac{\sqrt{d}}{2Q}>1} 1=\frac{1}{2}\tau\left(\frac{d}{4}\right);$$

又可见第三个和等于

$$\sum_{\substack{1\leqslant m<\sqrt{d},\ m\equiv d\,(\mathrm{mod}\,2)\\ 1\leqslant Q\mid\frac{d-m^2}{4},\ \frac{\sqrt{d}-m}{2Q}>1}} 1\ ,$$

这样就得到了

$$|\mathfrak{M}|=\frac{1}{2}\sum_{\substack{|m|<\sqrt{d},\ m\equiv d\,(\mathrm{mod}\ 2)\\ 1\leqslant Q\mid\frac{d-m^2}{4}}} 1=\frac{1}{2}\sum_{\substack{|m|<\sqrt{d}\\ m\equiv d\,(\mathrm{mod}\ 2)}}\tau\left(\frac{d-m^2}{4}\right),$$

这就证明了(1)。

再来证明(2)：由上述已证明的断言，定义1.1之后指出的ω相似于$\beta=\dfrac{-b+\sqrt{d}}{2a}$的充要条件是它们的简单连分数展开式从有限项以后完全相同，引理1.5以及引理1.8，即知ω的半单连分数展开式的基本周期如下所述：

当k为奇时，为：

$$\overline{a_{k-1}+2,\ \underbrace{2,\ \cdots,\ 2}_{a_{k-2}-1\text{个}},\ a_{k-3}+2,\ \cdots,\ \underbrace{2,\ \cdots,\ 2}_{a_1-1\text{个}},\ a_k+2,}$$
$$\overline{\underbrace{2,\ \cdots,\ 2}_{a_{k-1}-1\text{个}},\ \cdots,\ a_1+2,\ \underbrace{2,\ \cdots,\ 2}_{a_k-1\text{个}},}$$

或者为它的任一个轮换，这时长度为$\sum\limits_{n=1}^{k}a_n$；

当k为偶时，为：

$$\overline{a_{k-1}+2,\ \underbrace{2,\ \cdots,\ 2}_{a_{k-2}-1\text{个}},\ a_{k-3}+2,\ \cdots,\ \underbrace{2,\ \cdots,\ 2}_{a_2-1\text{个}},\ a_1+2,\ \underbrace{2,\ \cdots,\ 2}_{a_k-1\text{个}},}$$

或者为它的任一个轮换，这时长度为$\sum\limits_{\substack{1\leqslant n\leqslant k\\ n\text{偶}}}a_n$，以及

$\overline{a_k+2,\ \underbrace{2,\ \cdots,\ 2}_{a_{k-1}-1\text{个}},\ a_{k-2}+2,\ \cdots,\ a_2+2,\ \underbrace{2,\ \cdots,\ 2}_{a_1-1\text{个}},}$ 或者为它的

任一个轮换，这时长度为 $\sum\limits_{\substack{1\leq n\leq c\\ n奇}} a_n$。

由此可见，无论在 k 为奇或为偶的情况下，均有 $|\mathfrak{M}_\alpha|=\sum\limits_{n=1}^{k}a_n$。这就证明了(2)。

附记 由上述证明了的结论及引理1.5，即知有

$$|\mathfrak{M}_\alpha|=|\mathfrak{M}_\beta|,\ 若\ \alpha=\frac{b+\sqrt{d}}{2a},\ \beta=\frac{-b+\sqrt{d}}{2a}.$$

最后再来证明(3)。由(2)可知，为证明(3)，只需证明(3)的右边的集合中的每个 $\dfrac{P+\sqrt{d}}{2Q}$ 均属于 $\mathfrak{M}$，同时又都是约化的，相似于 β，并且相应于不同的参数 t，n 的 $\dfrac{P+\sqrt{d}}{2Q}$ 是不相同的。首先对每个这样的 $\dfrac{P+\sqrt{d}}{2Q}$，由定义，有

$$P=2Q-(P_{n+1}-2tQ_n),$$

$$4Q_nQ=4Q_nQ_{n+1}+4tQ_nP_{n+1}-4t^2Q_n^2=d-(2Q-P)^2, \quad (1.50)$$

其中用到 $P_{n+1}^2+4Q_nQ_{n+1}=d$。于是得到

$$4Q\,|\,d-P^2,\ 故\ \frac{P+\sqrt{d}}{2Q}\in\mathfrak{M}\ 如其约化。$$

又由定义，引理1.1与引理1.2，即知有

$$Q=Q_{n+1}+tP_{n+1}-t^2Q_n=Q_n\left(\frac{\sqrt{d}+P_{n+1}}{2Q_n}-t\right)\cdot\left(\frac{\sqrt{d}-P_{n+1}}{2Q_n}+t\right)>0.$$

于是 $Q\geq1$。再由(1.50)，即得

$$-\sqrt{d}<2Q-P<\sqrt{d},$$

从而有

$$\frac{P-\sqrt{d}}{2Q}<1<\frac{P+\sqrt{d}}{2Q},\ Q\geq1. \quad (1.51)$$

又由(1.50)可得

$$d=P^2+4Q(Q-P+Q_n). \quad (1.52)$$

另外由定义，引理1.1与引理1.2，可知有

$$Q-P+Q_n=Q_nt^2-(2Q_n+P_{n+1})t+Q_n-Q_{n+1}+P_{n+1}$$
$$=Q_n\left(t-1-\frac{\sqrt{d}+P_{n+1}}{2Q_n}\right)\left(t-1+\frac{\sqrt{d}-P_{n+1}}{2Q_n}\right)<0,$$

由此及 (1.52)，即得

$$P>Q+Q_n>0,\ d<P^2,\ \sqrt{d}<P,$$

从而得到

$$0<\frac{P-\sqrt{d}}{2Q}<1<\frac{P+\sqrt{d}}{2Q}.$$

其中用到(1.51)。这样$\dfrac{P+\sqrt{d}}{2Q}$是约化的。

再用引理1.1，可知有

$$\frac{1}{\dfrac{\sqrt{d}+P}{2Q}-1}=\frac{2Q}{\sqrt{d}+P-2Q}=\frac{\sqrt{d}+2Q-P}{2Q_n}$$
$$=\frac{\sqrt{d}+P_{n+1}-2Q_nt}{2Q_n}=\left[a_n-t,\ \frac{\sqrt{d}+P_n}{2Q_{n-1}}\right]$$
$$(n\geqslant 1).\qquad(1.53)$$

以上第二步还用了(1.50)。这样由引理1.5即知$\dfrac{\sqrt{d}+P}{2Q}$相似于β。

再设$\dfrac{P+\sqrt{d}}{2Q}$既相应于参数t、n，又相应于参数s、m，其中$1\leqslant n,\ m\leqslant k,\ 1\leqslant t\leqslant a_n,\ 1\leqslant s\leqslant a_m$。我们来证明$n=m,\ t=s$。

由定义以及(1.53)，可知有

$$a_n-t+\frac{\sqrt{d}-P_n}{2Q_n}=\frac{1}{\dfrac{\sqrt{d}+P}{2Q}-1}=a_m-s+\frac{\sqrt{d}-P_m}{2Q_m},$$

于是分别比较整数部分与小数部分，即得

$$a_n-t=a_m-s,\ \frac{\sqrt{d}-P_n}{2Q_n}=\frac{\sqrt{d}-P_m}{2Q_m}\ \text{即}\ Q_n=Q_m,\ P_n=P_m,$$

由此即得$n=m$，因此也有$t=s$。完全证明了所需的结论。这样完成了(3)的证明。引理证毕。

1.3 奇异连分数

定义 1.3 设 θ 为一个实的二次无理数，θ' 为 θ 所满足的有理系数二次方程的另一个根。满足条件

$$\theta>2,\quad \frac{1-\sqrt{5}}{2}<\theta'<\frac{3-\sqrt{5}}{2}$$

的 θ，称为是 H-约化的。

这个定义是 Hurwitz 引进的。

对一个 H-约化的实二次无理数 θ，我们如下地来定义它的奇异连分数。

令 $\theta_0=\theta$。对 $n\geqslant 0$，归纳地定义 θ_n 如下：设 θ_n 已是 H-约化的实二次无理数，即它满足

$$\theta_n>2,\ \frac{1-\sqrt{5}}{2}<\theta_n'<\frac{3-\sqrt{5}}{2}.$$

命

$$\theta_{n+1}=\begin{cases}\dfrac{1}{\{\theta_n\}}, & \text{如}\{\theta_n\}<\dfrac{1}{2};\\[2ex] \dfrac{1}{1-\{\theta_n\}}, & \text{如}\{\theta_n\}>\dfrac{1}{2},\end{cases}\tag{1.54}$$

这里 $\{x\}$ 表示 x 的小数部分。我们先来证明 θ_{n+1} 也是 H-约化的。命

$$t_n=\begin{cases}[\theta_n],\\ [\theta_n]+1,\end{cases}\quad \mu_{n+1}=\begin{cases}1,\\ -1,\end{cases}\quad \text{如}\ \{\theta_n\}\begin{cases}<\dfrac{1}{2};\\[2ex] >\dfrac{1}{2}.\end{cases}$$

则有

$$\theta_n=t_n+\frac{\mu_{n+1}}{\theta_{n+1}},\quad \theta_n'=t_n+\frac{\mu_{n+1}}{\theta_{n+1}'},$$

以及

$$t_n\geqslant 2,\ \text{并且}\ t_n\geqslant 3,\ \text{若}\ \mu_{n+1}=-1.$$

由定义(1.54)即知 $\theta_{n+1}>2$。

当 $\mu_{n+1}=1$ 时，由 $\theta_{n+1}'=(\theta_n'-t_n)^{-1}$ 以及 $\theta_n'<\dfrac{3-\sqrt{5}}{2}<2\leqslant$

t_n，即知 θ'_{n+1} 与 θ'_n-t_n 均是负的。又 $t_n-\theta'_n>2-\frac{3-\sqrt{5}}{2}$ $=\frac{1+\sqrt{5}}{2}$，从而有

$$0>\theta'_{n+1}=\frac{-1}{t_n-\theta'_n}>-\frac{2}{1+\sqrt{5}}=\frac{1-\sqrt{5}}{2}.$$

即已证明 $\mu_{n+1}=1$ 时，θ_{n+1} 是 H-约化的。

当 $\mu_{n+1}=-1$ 时，由 $\theta'_{n+1}=(t_n-\theta'_n)^{-1}$ 以及 $t_n-\theta'_n>3-\frac{3-\sqrt{5}}{2}=\frac{3+\sqrt{5}}{2}$，得到

$$0<\theta'_{n+1}<\frac{2}{3+\sqrt{5}}=\frac{3-\sqrt{5}}{2}.$$

即知 $\mu_{n+1}=-1$ 时，θ_{n+1} 仍是 H-约化的。

总之，已证明了 θ_{n+1} 也是 H-约化的。把上述步骤一直做下去可得：

$$\theta_n=t_n+\frac{\mu_{n+1}}{\theta_{n+1}},\quad \theta'_n=t_n+\frac{\mu_{n+1}}{\theta'_{n+1}}\quad (n\geqslant 0); \tag{1.55}$$

$$t_n\in\mathbb{Z},\ t_n\geqslant 2,\ \mu_{n+1}=\pm 1\quad (n\geqslant 0); \tag{1.56}$$

$$t_n\geqslant 3,\ 如\ \mu_{n+1}=-1\quad (n\geqslant 0); \tag{1.57}$$

$$\theta_n\ 均为\ H\text{-}约化的\quad (n\geqslant 0); \tag{1.58}$$

$$\mu_n\theta'_n<0\quad (n\geqslant 1). \tag{1.59}$$

我们记为 $\theta=\{t_0,\ \mu_1t_1,\ \mu_2t_2,\ \cdots\}$.

引理 1.10 每一个不相似于 $\frac{1+\sqrt{5}}{2}$ 的实二次无理数 ω 均相似于一个 H-约化的实二次无理数。

证明 不妨设 ω 的简单连分数展开式为

$$\omega=[\overline{a_0,\ \cdots,\ a_{k-1}}],$$

其中 $a_n\geqslant 1(n\geqslant 0)$，$\overline{a_0,\ \cdots,\ a_{k-1}}$ 为基本周期。如有 $a_n=1(n\geqslant 0)$，则 $\omega=[\bar{1}]=\frac{1+\sqrt{5}}{2}$，与假设矛盾。于是存在一个 n，$0\leqslant n\leqslant k-1$，使 $a_n\geqslant 2$。这样由引理 1.1 与引理 1.2 即知（并用那里的符号）

$$\omega_n=\frac{P_n+\sqrt{d}}{2\Theta_n}>2,\quad \omega_n'=\frac{P_n-\sqrt{d}}{2\Theta_n}<0.$$

如有 $\omega_n'<\frac{1-\sqrt{5}}{2}$，则由引理 1.2 有

$$\frac{3-\sqrt{5}}{2}>1+\omega_n'=\frac{2\Theta_n+P_n-\sqrt{d}}{2\Theta_n}>0.$$

因此 ω_n 或 $1+\omega_n$ 是 H-约化的，引理证毕。

引理 1.11 设有理整数 a、b、c，满足 $|b|\leqslant a\leqslant c$，且 $d=b^2+4ac$ 不是完全平方。设 $\alpha=\frac{b+\sqrt{d}}{2a}$ 的简单连分数展开式为

$$\alpha=[a_0,\overline{a_1,\ \cdots,\ a_k}],$$

其中 $\overline{a_1,\ \cdots,\ a_k}$ 为基本周期，再设 α 的第 n 个完全商

$$\alpha_n=\frac{P_n+\sqrt{d}}{2Q_n}$$

满足条件

$$Q_n\geqslant Q_0\quad (n\geqslant 0).$$

最后设 α 不相似于 $\frac{1+\sqrt{5}}{2}$。

则有

(1) $a_k\geqslant 2$;

(2) 令

$$\theta=[\overline{a_k,\ a_1\ \cdots,\ a_{k-1}}]+\delta_0,$$

这里 $\delta_0=0$ 或 1 依 l 为奇或偶而定，其中 l 由下列条件决定之：

$a_{k-1}=a_{k-2}=\cdots=a_{k-l+1}=1$，而 $a_{k-l}\geqslant 2$，这里出现的 a_0 认为是 a_k。

那么 θ 是 H-约化的。且 θ 的奇异连分数展开式可如下得出：命

$$\theta_0=\theta=\alpha_k+\delta_0.$$

设对 $n\geqslant 0$，已有 $\theta_n=\alpha_m+\delta_n$ 为 H-约化的，其中 $\delta_n=0$ 或 1，$m\geqslant 0$，这里可能出现的 a_0 认为是 a_k。那么

$$\theta_{n+1}=\begin{cases}\alpha_{m+1}, & \text{如 } a_{m+1}\geqslant 2;\\ 1+\alpha_{m+2}=\alpha_{m+1}\alpha_{m+2}, & \text{如 } a_{m+1}=1,\end{cases}$$

是 H-约化的，且有

$$t_n=\begin{cases}a_m+\delta_n,\\a_m+\delta_n+1,\end{cases}\quad \mu_{n+1}=\begin{cases}1,\\-1,\end{cases}\text{如 }a_{m+1}\begin{cases}\geqslant 2;\\=1,\end{cases}$$

(其中可能出现的 a_0 认为是 a_k)它们使

$$\theta_n=t_n+\frac{\mu_{n+1}}{\theta_{n+1}}.$$

从而得到 θ 的奇异连分数展开式：

$$\theta=\{\overline{\mu_0 t_0,\ \mu_1 t_1,\ \cdots,\ \mu_{k-1}t_{k-1}}\},\ \mu_0=\mu_k,\ t_0=t_k,$$

这个记号的意义如下：

$$\theta_0=\theta,\ \theta_n=t_n+\frac{\mu_{n+1}}{\theta_{n+1}}\ (n\geqslant 0),\ t_{n+k}=t_n(n\geqslant 0),$$

$$\mu_{n+k}=\mu_n(n\geqslant 0).$$

$\overline{\mu_0 t_0,\ \mu_1 t_1,\ \cdots,\ \mu_{k-1}t_{k-1}}$ 称为基本周期，它的长度 K 满足

$$K\leqslant k,$$

即 θ 的奇异连分数是纯循环的，并且循环节的长度小于等于 k。

证明　首先来证明 $a_k\geqslant 2$。

先看 $b\geqslant 0$ 的情况：当 $b=0$ 时，由引理 1.3 即知 $a_k=2a_0$，而 $a_0\geqslant 1$，故得 $a_k\geqslant 2$。故可设 $b>0$。用反证法：即：如有 $a_k=1$，则必有 $\alpha\sim\frac{1+\sqrt{5}}{2}$，这样就得出矛盾，在 $a_k=1$ 的假定下，有 $k\geqslant 2\left(否则, \alpha\sim\frac{1+\sqrt{5}}{2}\right)$。由引理 1.3 之前的计算可知，此时必有

$$a_0=1,\ \sqrt{d}<2a+b, \tag{1.60}$$

后一不等式的证明用了 $a_k=a_0+\left[\frac{\sqrt{d}-b}{2a}\right]$。并可有

$$Q_0=a,\ P_0=b,\ P_1=2a-b,\ Q_1=\frac{d-P_1^2}{4Q_0}=c-a+b \tag{1.61}$$

我们来证明 $a_1=1$。由假设及(1.61)有

$$c-a+b=Q_1\geqslant Q_0=a,\ 故\ c\geqslant 2a-b. \tag{1.62}$$

从而由(1.60)～(1.62)可得

$$\frac{\sqrt{d}+P_1}{2Q_1}-2=\frac{\sqrt{d}+P_1-4Q_1}{2Q_1},$$

其分子为$\sqrt{d}+6a-5b-4c<8a-4b-4c=4(2a-b-c)\leqslant 0$，这证明了$a_1=1$。从而$k\geqslant 3\left(否则\ \alpha\sim\frac{1+\sqrt{5}}{2}\right)$。

由假设有

$$a=Q_0\leqslant Q_2=Q_0+a_1P_1-a_1^2Q_1=Q_0+P_1-Q_1=4a-2b-c,$$

故有

$$c\leqslant 3a-2b. \tag{1.63}$$

这样用到(1.60)，(1.61)，(1.63)，$a_1=1$以及

$$Q_2=Q_0+P_1-Q_1,\ P_2=2a_1Q_1-P_1=2Q_1-P_1.$$

即知下式

$$\frac{P_2+\sqrt{d}}{2Q_2}-2=\frac{\sqrt{d}+P_2-4Q_2}{2Q_2}$$

的分子为$\sqrt{d}+6c-2a+11b<6c-18a+12b=6(c-3a+2b)\leqslant 0$，故得$a_2=1$，$k\geqslant 4$。

一般的，设已有

$$Q_n=\frac{1}{5}(2-(-1)^nL_{2n})c+\frac{1}{5}(2+(-1)^nL_{2n+2})a$$
$$+\frac{1}{5}(1-(-1)^nL_{2n+1})b\quad(1\leqslant n\leqslant m), \tag{1.64}$$

$$P_n=\frac{1}{5}(2+(-1)^n2L_{2n-1})c+\frac{1}{5}(2-(-1)^n2L_{2n+1})a$$
$$+\frac{1}{5}(1+(-1)^n2L_{2n})b\quad(1\leqslant n\leqslant m), \tag{1.65}$$

$$a_n=1\quad(0\leqslant n\leqslant m), \tag{1.66}$$

$$k\geqslant m+2, \tag{1.67}$$

其中L_u是Lucas数，即它们满足

$$L_1=1,\ L_2=3,\ L_n=L_{n-1}+L_{n-2}\ (n\geqslant 3).$$

由以上所证，(1.64)～(1.67)已对$m=2$成立。我们要证明m换成$m+1$后，(1.64)～(1.67)仍成立。首先指出易有

$$L_n^2-L_{n-1}L_{n+1}=5(-1)^n\quad(n\geqslant 2). \tag{1.68}$$

由引理 1.1 及(1.64)~(1.66)有

$$P_{m+1}=2a_mQ_m-P_m=2Q_m-P_m=\frac{1}{5}(2-(-1)^m2L_{2m+1})c$$
$$+\frac{1}{5}(2+(-1)^mL_{2m+3})a+\frac{1}{5}(1-(-1)^m2L_{2m+2})b, \tag{1.69}$$

$$\begin{aligned}Q_{m+1}&=Q_{m-1}-a_m^2Q_m+a_mP_m=Q_{m-1}-Q_m+P_m\\&=\frac{1}{5}(2+(-1)^m(L_{2m-2}+L_{2m}+2L_{2m-1}))c\\&\quad+\frac{1}{5}(2-(-1)^m(L_{2n}+L_{2m-2}+2L_{2m+1}))a\\&\quad+\frac{1}{5}(1+(-1)^m(L_{2m-1}+L_{2m+1}+2L_{2m}))b\\&=\frac{1}{5}(2-(-1)^{m+1}L_{2m+2})c\\&\quad+\frac{1}{5}(2+(-1)^{m+1}L_{2m+4})a\\&\quad+\frac{1}{5}(1-(-1)^{m+1}L_{2m+3})b,\end{aligned} \tag{1.70}$$

因此(1.64), (1.65)已对 $m+1$ 成立。剩下来只需证明 $a_{m+1}=1$。如有 $a_{n+1}\geqslant 2$, 则由

$$\frac{\sqrt{d}+P_{m+1}}{2Q_{m+1}}>a_{m+1}\geqslant 2$$

以及 (1.60), 即有

$$2a+b>\sqrt{d}>4Q_{m+1}-P_{m+1}.$$

结合(1.69)与(1.70)有

$$(3-(-1)^{m+1}L_{2m+4})c+(-2+(-1)^{m+1}L_{2m+6})a$$
$$+(-1-(-1)^{m+1}L_{2m+5})b<0, \tag{1.71}$$

再由 $Q_{n+1}\geqslant Q_0=a$ 的假设及(1.70), 即知

$$(2-(-1)^{m+1}L_{2m+2})c+(-3+(-1)^{m+1}L_{2m+4})a$$
$$+(1-(-1)^{m+1}L_{2m+3})b\geqslant 0, \tag{1.72}$$

用 (1.68), 计算 $(L_{2m+4}-(-1)^m2)\times(1.72)-(L_{2m+3}+(-1)^m)\times((1.71)-(1.72))$即得

$$0>0,$$

这个矛盾证明了 $a_{m+1}=1$。因此 (1.64)~(1.67) 对 $m+1$ 也成立。所以由归纳法原理即知，我们已证明了

$$a_0=a_1=\cdots=a_k=1,$$

从而有 $\alpha=[\bar{1}]=\frac{1+\sqrt{5}}{2}$，这与 α 不相似于 $\frac{1+\sqrt{5}}{2}$ 的假设矛盾。这样证明了当 $b\geqslant 0$ 时，有 $a_k\geqslant 2$。在 $b<0$ 时，由于引理1.5，我们知道

$$\frac{-b+\sqrt{d}}{2a}=[a_k-a_0, \overline{a_{k-1}, a_{k-2}, \cdots, a_1, a_k}],$$

这时 $-b>0$，再由引理 1.5，类似的假设

$$Q_n\geqslant Q_0\ (n\geqslant 0)$$

也是成立的，故由上面的证明可得 $a_k\geqslant 2$。

因此，不论 b 是零、正或负，都已证明了 $a_k\geqslant 2$。

由已证明的 $a_k\geqslant 2$，即知有

$$\alpha_k>2,\ -1<\alpha_k'<0。$$

所以为证明 θ 是 H-约化的，只需证明

$$\alpha_k'\begin{cases}>\dfrac{1-\sqrt{5}}{2}, & \text{如 } l \text{ 奇;}\\[2ex] <\dfrac{1-\sqrt{5}}{2}, & \text{如 } l \text{ 偶。}\end{cases}$$

命

$$\eta_n=-\frac{1}{\alpha_n'}\ (n\geqslant 0),$$

其中可能出现的 α_0 认为是 α_k。那么有 $\eta_n>1$，并且由 $\alpha_n=a_n+\alpha_{n+1}^{-1}$ 可得

$$\eta_{n+1}=a_n+\frac{1}{\eta_n}\quad (n\geqslant 0)。\tag{1.73}$$

于是只需证明

$$\eta_k\begin{cases}>\dfrac{\sqrt{5}+1}{2}, & \text{如 } l \text{ 奇;}\\[2ex] <\dfrac{\sqrt{5}+1}{2}, & \text{如 } l \text{ 偶。}\end{cases}\tag{1.74}$$

反复运用(1.73)可得

$$\eta_k-\frac{\sqrt{5}+1}{2}=a_{k-1}+\frac{1}{\eta_{k-1}}-\frac{\sqrt{5}+1}{2}$$

$$=\frac{1}{\eta_{k-1}}-\frac{\sqrt{5}-1}{2}=\frac{1}{\eta_{k-1}}-\frac{1}{\frac{\sqrt{5}+1}{2}}$$

$$=\frac{-\left(\eta_{k-1}-\frac{\sqrt{5}+1}{2}\right)}{\frac{\sqrt{5}+1}{2}\eta_{k-1}}=\cdots$$

$$=\frac{(-1)^{l-1}\left(\eta_{k-l+1}-\frac{\sqrt{5}+1}{2}\right)}{\left(\frac{\sqrt{5}+1}{2}\right)^{l-1}\eta_{k-1}\eta_{k-2}\cdots\eta_{k-l+1}},\qquad(1.75)$$

以上用了 l 的定义。仍由 l 的定义可得

$$\eta_{k-l+1}-\frac{\sqrt{5}+1}{2}=a_{k-l}+\frac{1}{\eta_{k-l}}$$

$$-\frac{\sqrt{5}+1}{2}>\frac{3-\sqrt{5}}{2}>0,$$

由此及(1.75)，立即得到所欲证明的(1.74)。从而也就证明了 θ 是 H-约化的。

又　$\theta_0=\delta_0+\alpha_k=\delta_0+a_k+\dfrac{1}{\alpha_1}$. 当 $a_1\geqslant 2$ 时，有 $\alpha_1>2$。再由 $\theta_0=\theta$ 是 H-约化的，即有

$$-\frac{1}{\alpha_1'}=\delta_0+a_k-\theta_0'>2-\frac{3-\sqrt{5}}{2}=\frac{1+\sqrt{5}}{2},\quad 故\ \frac{1-\sqrt{5}}{2}$$

$<\alpha_1'<0$，即 $a_1\geqslant 2$ 时，α_1 是 H-约化的。

$a_1=1$ 时，$\alpha_1<2$，且有

$$\alpha_1=1+\frac{1}{\alpha_2},$$

从而

$$\theta_0=\delta_0+a_k+1-\frac{1}{1+\alpha_2}.$$

令 $\theta_1=1+\alpha_2$，则有 $\theta_1>2$，以及

$$-\frac{1}{\theta_1'}=\theta_0'-(\delta_0+\alpha_k+1)<\frac{3-\sqrt{5}}{2}-3$$
$$=-\frac{3+\sqrt{5}}{2}，故 0<\theta_1'<\frac{3-\sqrt{5}}{2},$$

即 $\theta_1=1+\alpha_2=\alpha_1\alpha_2$ 是H-约化的。

循此以往，即得引理中所叙述的 θ 的奇异连分数展开式。

为证明 θ 的奇异连分数展开式是纯循环的，只需证明存在一个正整数 m，使 $\theta_m=\theta_0$。根据上述证明过程，可知存在一个正整数 n，使 $\theta_n=\delta_n+\alpha_{k-l}$，其中 $\delta_n=0$ 或 1。再由 l 的定义可知：

如 l 为奇数，则 $\theta_{n+\frac{l-1}{2}+1}=\alpha_k=\delta_0+\alpha_k=\theta_0$；

如 l 为偶数，则 $\theta_{n+\frac{l-2}{2}+1}=1+\alpha_k=\delta_0+\alpha_k=\theta_0$，

即证明了取

$$m=\begin{cases}n+\dfrac{l-1}{2}+1, & 如\ l\ 奇;\\[2mm] n+\dfrac{l-2}{2}+1, & 如\ l\ 偶.\end{cases}$$

即有 $\theta_m=\theta_0$。因此 θ 的奇异连分数展开式是纯循环的。同时可知循环节的长度 $K\leqslant k$。这里我们应该补充证明以下两点。第一点，对同一个 $u(\bmod k)$，不可能有不同的 θ_n 与 θ_m 使

$$\theta_n=\alpha_u 与 \theta_m=1+\alpha_u.$$

这是因为由前者得到 $\frac{1-\sqrt{5}}{2}<\alpha_u'<0$，而由后者得到 $0<1+\alpha_u'<\frac{3-\sqrt{5}}{2}$，即 $-1<\alpha_u'<\frac{1-\sqrt{5}}{2}$，产生了矛盾。第二点，如有

$$\theta_n=\delta_n+\alpha_u=\delta_m+\alpha_v,$$

其中 δ_n、$\delta_m=0$，1，使 θ_n 为H-约化的，则必有 $\delta_n=\delta_m$，和 $u\equiv v\ (\bmod k)$。这是因为当 $\delta_n\neq\delta_m$ 时，不妨设 $\delta_n=0$ 而 $\delta_m=1$，那么有

$$\sqrt{d}>P_u=2Q_v+P_v>\sqrt{d},$$

产生矛盾，从而 $\delta_n=\delta_m$。因此 $\alpha_u=\alpha_v$，故 $u\equiv v\ (\bmod k)$，

引理得证。

附记 $Q_n \geqslant Q_0 (n \geqslant 0)$ 的假设相当于条件

$$a = \min_{\substack{m,n\in\mathbf{Z}\\(m,n)\neq(0,0)}} |am^2 - bmn - cn^2|,$$

所以这一假设没有失去一般性，虽然找出如上的极小值是一件不容易的事，但理论上总可以办到，在具体情况时，可通过有限步办到。

1.4 例 子

我们在本节中给出一些实二次无理数连分数展开式的例子。在最后，我们还要说明为什么只给出这十八个例子。

例 1 $d = S^2R^2 + R$，S、R 为正奇数，且 $R \equiv 3 \pmod 4$。$a = 1$，$b = 0$，$c = \frac{d}{4}$。$\alpha = \frac{\sqrt{d}}{2}$。

(a) $S = 1$ 时，α 的简单连分数展开式列表如下：

n	0	1	2	3	4
a_n	$\frac{R-1}{2}$	1	2	1	$R-1$
P_n	0	$R-1$	$\frac{R+1}{2}$	$\frac{R+1}{2}$	$R-1$
Q_n	1	$\frac{3R-1}{4}$	$\frac{R+1}{4}$	$\frac{3R-1}{4}$	1

$1+\alpha_k$ 的奇异连分数展开式为

$$\theta_0 = R + 1 - \frac{1}{\theta_1} = \frac{R+1+\sqrt{d}}{2},\ \theta_1 = 4 - \frac{1}{\theta_0} = \frac{R+1+\sqrt{d}}{(R+1)/2}.$$

(b) $S \geqslant 3$ 时，α 的简单连分数展开式列表如下：

n	0	1	2	3	4	5	6
a_n	$\frac{RS-1}{2}$	1	1	$S-1$	1	1	$RS-1$
P_n	0	$RS-1$	$\frac{R+1}{2}$	$R(S-1)$	$R(S-1)$	$\frac{R+1}{2}$	$RS-1$
Q_n	1	$\frac{2RS+R-1}{4}$	$\frac{2RS-R+1}{4}$	R	$\frac{2RS-R+1}{4}$	$\frac{2RS+R-1}{4}$	1

α_k 的奇异连分数展开式为

$$\theta_0 = RS - \frac{1}{\theta_1} = \frac{RS-1+\sqrt{d}}{2},$$

$$\theta_1 = 2 + \frac{1}{\theta_2} = \frac{RS+1+\sqrt{d}}{(2RS-R+1)/2},$$

$$\theta_2 = S - \frac{1}{\theta_3} = \frac{R(S-1)+\sqrt{d}}{2R},$$

$$\theta_3 = 2 + \frac{1}{\theta_0} = \frac{RS+R+\sqrt{d}}{(2RS+R-1)/2}.$$

例 2 $d=4S^2R^2+4R$, S、R 是正奇数, $R\equiv 1 \pmod 4$. $a=1$, $b=0$, $c=R^2S^2+R$. $\alpha=\frac{\sqrt{d}}{2}$的简单连分数展开式如下表:

n	0	1	2
a_n	RS	$2S$	$2RS$
P_n	0	$2RS$	$2RS$
Q_n	1	R	1

α_k 的奇异连分数展开式为

$$\theta_0 = 2RS + \frac{1}{\theta_1} = \frac{2RS+\sqrt{d}}{2},\quad \theta_1 = 2S + \frac{1}{\theta_0} = \frac{2RS+\sqrt{d}}{2R}.$$

例 3 $d=S^2R^2-R$, S、R 是正奇数, $R\equiv 1 \pmod 4$. $a=1$, $b=0$, $c=\frac{d}{4}$, $\alpha=\frac{\sqrt{d}}{2}$.

(a) $S=1$ 时, 这时$R\geqslant 5$, $\alpha=\frac{\sqrt{d}}{2}$的简单连分数展开式列表如下:

n	0	1	2
a_n	$\frac{R-1}{2}$	4	$R-1$
P_n	0	$R-1$	$R-1$
Q_n	1	$\frac{R-1}{4}$	1

α_k 的奇异连分数展开式为

$$\theta_0 = R-1+\frac{1}{\theta_1} = \frac{R-1+\sqrt{d}}{2},\ \theta_1 = 4+\frac{1}{\theta_0} = \frac{R-1+\sqrt{d}}{(R-1)/2}.$$

(b) $S\geqslant 3$ 时，α 的简单连分数展开式列表如下：

n	0	1	2	3	4
a_n	$\frac{RS-1}{2}$	2	$S-1$	2	$RS-1$
P_n	0	$RS-1$	$R(S-1)$	$R(S-1)$	$RS-1$
Q_n	1	$\frac{2RS-R-1}{4}$	R	$\frac{2RS-R-1}{4}$	1

α_k 的奇异连分数展开式为 $\{\overline{RS-1,\ 2,\ S-1,\ 2}\}$。

例 4　$d=4R^2S^2-4R$, S、R 是正奇数，$R\equiv 3 \pmod 4$。$a=1$, $b=0$, $c=R^2S^2-R$, $\alpha=\frac{\sqrt{d}}{2}$。

(a) $S=1$ 时，α 的简单连分数展开式如下表：

n	0	1	2
a_n	$R-1$	2	$2(R-1)$
P_n	0	$2(R-1)$	$2(R-1)$
Q_n	1	$R-1$	1

α_k 的奇异连分数为 $\{\overline{2R-2,\ 2}\}$。

(b) $S\geqslant 3$ 时，α 的简单连分数展开式如下表：

n	0	1	2	3	4
a_n	$RS-1$	1	$2(S-1)$	1	$2(RS-1)$
P_n	0	$2(RS-1)$	$2R(S-1)$	$2R(S-1)$	$2(RS-1)$
Q_n	1	$2RS-R-1$	R	$2RS-R-1$	1

$1+\alpha_k$ 的奇异连分数展开式为

$$\theta_0=2RS-\frac{1}{\theta_1}=\frac{2RS+\sqrt{d}}{2},\quad \theta_1=2S-\frac{1}{\theta_0}=\frac{2RS+\sqrt{d}}{2R}.$$

例 5　$d=4R^2S^2+8R$, R、S 是正奇数。$a=1$, $b=0$, $c=R^2S^2+2R$, $\alpha=\frac{\sqrt{d}}{2}$。

(a) $S=1$ 时，α 的简单连分数展开式如下表：

n	0	1	2
a_n	R	1	$2R$

P_n	0	$2R$	$2R$
Q_n	1	$2R$	1

$1+\alpha_k$ 的奇异连分数为

$$\theta_0=2R+2-\frac{1}{\theta_0}=\frac{2R+2+\sqrt{d}}{2}.$$

(*b*) $S\geqslant 3$ 时，α 的简单连分数展开式如下表：

n	0	1	2
a_n	RS	S	$2RS$
P_n	0	$2RS$	$2RS$
Q_n	1	$2R$	1

α_k 的奇异连分数为 $\{\overline{2RS,\ S}\}$。

例 6　$d=4R^2S^2-8R$, R、S 是正奇数。$a=1$, $b=0$, $c=R^2S^2-2R$。$\alpha=\frac{\sqrt{d}}{2}$.

(*a*) $S=1$, 此时 $R\geqslant 3$。α 的简单连分数列表如下：

n	0	1	2
a_n	$R-2$	1	$2(R-2)$
P_n	0	$2(R-2)$	$2(R-2)$
Q_n	1	$2(R-2)$	1

$1+\alpha_k$ 的奇异连分数是

$$\theta_0=2(R-1)-\frac{1}{\theta_0}=\frac{2(R-1)+\sqrt{d}}{2}.$$

(*b*) $S\geqslant 3$ 时，α 的简单连分数如下表：

n	0	1	2	3	4
a_n	$RS-1$	1	$S-2$	1	$2(RS-1)$
P_n	0	$2(RS-1)$	$2R(S-2)$	$2R(S-2)$	$2(RS-1)$
Q_n	1	$2RS-2R-1$	$2R$	$2RS-2R-1$	1

$1+\alpha_k$ 的奇异连分数为

$$\theta_0=2RS-\frac{1}{\theta_1}=\frac{2RS+\sqrt{d}}{2},\ \theta_1=S-\frac{1}{\theta_0}=\frac{2RS+\sqrt{d}}{4R}.$$

例 7 $d=R^2S^2+4R$, S、R 为正奇数。$a=b=1$, $c=\frac{d-1}{4}$,

$\alpha=\frac{1+\sqrt{d}}{2}$。$\alpha$ 的简单连分数如下表：

n	0	1	2
a_n	$\frac{SR+1}{2}$	S	SR
P_n	1	SR	SR
Q_n	1	R	1

$S=1$ 时，$1+\alpha_k$ 的奇异连分数为

$$\theta_0=R+2-\frac{1}{\theta_0}=\frac{R+2+\sqrt{d}}{2}.$$

$S\geqslant 3$ 时，α_k 的奇异连分数为 $\{\overline{SR,\ S}\}$。

例 8 $d=R^2S^2-4R$, R、S 是正奇数。$a=b=1$, $c=\frac{d-1}{4}$,

$\alpha=\frac{1+\sqrt{d}}{2}$.

(a) $S=1$ 时，α 的简单连分数如下表($R\geqslant 5$)：

n	0	1
a_n	$\frac{R-1}{2}$	$R-2$
P_n	1	$R-2$
Q_n	1	1

α_k 的奇异连分数为 $\{\overline{R-2}\}$。

(b) $S\geqslant 3$ 时，α 的简单连分数如下表：

n	0	1	2	3	4
a_n	$\frac{RS-1}{2}$	1	$S-2$	1	$RS-2$
P_n	1	$RS-2$	$R(S-2)$	$R(S-2)$	$RS-2$
Q_n	1	$RS-R-1$	R	$RS-R-1$	1

$1+\alpha_k$ 的奇异连分数为

$$\theta_0=RS-\frac{1}{\theta_1}=\frac{RS+\sqrt{d}}{2},\quad \theta_1=S-\theta_0=\frac{RS+\sqrt{d}}{2R}.$$

例 9 $d=4^M R^2 S^2+R$，R、S 是正奇数，$R\equiv 1 \pmod 4$，M 为正整数。$a=b=1$，$c=\dfrac{d-1}{4}$，$\alpha=\dfrac{1+\sqrt{d}}{2}$。

(a) $R=1$，但 M、S 不全为 1 时，α 的简单连分数列表如下：

n	0	1	2	3
a_n	$2^{M-1}S$	1	1	$2^M S-1$
P_n	1	$2^M S-1$	1	$2^M S-1$
Q_n	1	$2^{M-1}S$	$2^{M-1}S$	1

α_k 的奇异连分数为

$$\theta_0=2^M S-\frac{1}{\theta_1}=\frac{2^M S-1+\sqrt{d}}{2},$$

$$\theta_1=2+\frac{1}{\theta_0}=\frac{2^M S+1+\sqrt{d}}{2^M S}.$$

(b) $R\geqslant 5$ 时，α 的简单连分数如下表：

n	0	1	2	3
a_n	$2^{M-1}RS$	1	1	$2^M S-1$
P_n	1	$2^M RS-1$	$\dfrac{R+1}{2}$	$2^M RS-R$
Q_n	1	$2^{M-1}RS+\dfrac{R-1}{4}$	$2^{M-1}RS-\dfrac{R-1}{4}$	R

n	4	5	6
a_n	1	1	$2^M RS-1$
P_n	$2^M RS-R$	$\dfrac{R+1}{2}$	$2^M RS-1$
Q_n	$2^{M-1}RS-\dfrac{R-1}{4}$	$2^{M-1}RS+\dfrac{R-1}{4}$	1

当 M、S 不同时为 1 时，α_k 的奇异连分数为

$$\theta_0=2^M RS-\frac{1}{\theta_1}=\frac{2^M RS-1+\sqrt{d}}{2},$$

$$\theta_1=2+\frac{1}{\theta_2}=\frac{2^M RS+1+\sqrt{d}}{2^M RS-\dfrac{R-1}{2}},$$

$$\theta_2=2^MS-\frac{1}{\theta_3}=\frac{2^MRS-R+\sqrt{d}}{2R},$$

$$\theta_3=2+\frac{1}{\theta_0}=\frac{2^MRS+R+\sqrt{d}}{2^MRS+\dfrac{R-1}{2}};$$

而当 $M=S=1$ 时，$1+\alpha_k$ 的奇异连分数为

$$\theta_0=R+1-\frac{1}{\theta_1}=\frac{2R+1+\sqrt{d}}{2},\ \theta_1=3-\frac{1}{\theta_2}=\frac{2R+1+\sqrt{d}}{(R+1)/2},$$

$$\theta_2=3-\frac{1}{\theta_0}=\frac{R+\dfrac{R+1}{2}+\sqrt{d}}{(R+1)/2}.$$

例 10　$d=4^MR^2S^2-R$, R、S 是正奇数，$R\equiv3\pmod 4$，M正整数。$a=b=1$, $c=\dfrac{d-1}{4}$, $\alpha=\dfrac{1+\sqrt{d}}{2}$.

α 的简单连分数如下表：

n	0	1	2	3	4
a_n	$2^{M-1}RS$	2	2^MS-1	2	2^MRS-1
P_n	1	2^MRS-1	2^MRS-R	2^MRS-R	2^MRS-1
Q_n	1	$2^{M-1}RS-\dfrac{R+1}{4}$	R	$2^{M-1}RS-\dfrac{R+1}{4}$	1

当 $M=S=1$ 时，α_k 的奇异连分数为

$$\theta_0=R-1+\frac{1}{\theta_1}=\frac{R-1+\sqrt{d}}{2},\ \theta_1=3-\frac{1}{\theta_2}=\frac{R-1+\sqrt{d}}{(R-1)/2},$$

$$\theta_2=3+\frac{1}{\theta_0}=\frac{\dfrac{5R-1}{2}+\sqrt{d}}{(R-1)/2}.$$

而当 M、S 不同时为1时，α_k 的奇异连分数为

$$\{\overline{2^MRS-1,\ 2,\ 2^MS-1,\ 2}\}.$$

例 11　$d=4^{M+1}R^2S^2+8R$, R、S 是正奇数，M正整数，$a=1$, $b=0$, $c=4^MR^2S^2+2R$, $\alpha=\dfrac{\sqrt{d}}{2}$.

α 的简单连分数如下表：

n	0	1	2
a_n	$2^M RS$	$2^M S$	$2^{M+1}RS$
P_n	0	$2^{M+1}RS$	$2^{M+1}RS$
Q_n	1	$2R$	1

α_k 的奇异连分数为$\{\overline{2^{M+1}RS,\ 2^M S}\}$。

例 12 $d=4^{M+1}R^2S^2-8R$, R、S 是正奇数，M正整数，$a=1$, $b=0$, $c=4^M R^2S^2-2R$, $\alpha=\frac{\sqrt{d}}{2}$.

(a) $M=S=1$ 时，α 的简单连分数展开式如下表：

n	0	1	2
a_n	$2R-1$	2	$4R-2$
P_n	0	$4R-2$	$4R-2$
Q_n	1	$2R-1$	1

α_k 的奇异连分数为$\{\overline{4R-2,\ 2}\}$。

(b) $MS>1$时，α 的简单连分数展开式如下表：

n	0	1	2	3	4
a_n	$2^M RS-1$	1	$2^M S-2$	1	$2^{M+1}RS-2$
P_n	0	$2^{M+1}RS-2$	$2^{M+1}RS-4R$	$2^{M+1}RS-4R$	$2^{M+1}RS-2$
Q_n	1	$2^{M+1}RS-2R-1$	$2R$	$2^{M+1}RS-2R-1$	1

$1+\alpha_k$ 的奇异连分数为

$$\theta_0=2^{M+1}RS-\frac{1}{\theta_1}=\frac{2^{M+1}RS+\sqrt{d}}{2},$$

$$\theta_1=2^M S-\frac{1}{\theta_0}=\frac{2^{M+1}RS+\sqrt{d}}{4R}.$$

例 13 $d=4^M R^2S^2+2^m R$, R、S 是正奇数，$2\leqslant m\leqslant M$, $a=1$, $b=0$, $c=4^{M-1}R^2S^2+2^{m-2}R$, $\alpha=\frac{\sqrt{d}}{2}$.

α 的简单连分数展开式如下表：

n	0	1	2
a_n	$2^{M-1}RS$	$2^{M-m+2}RS$	$2^M RS$

P_n	0	$2^M RS$	$2^M RS$
Q_n	1	$2^{m-2}R$	1

α_n的奇异连分数为$\{\overline{2^M RS,\ 2^{M-m+2}RS}\}$。

例 14 $d=4^M R^2 S^2-2^m R$, R、S是正奇数，$2\leqslant m\leqslant M$, $a=1$, $b=0$, $c=4^{M-1}R^2S^2-2^{m-2}R$, $\alpha=\frac{\sqrt{d}}{2}$。$\alpha$的简单连分数展开式如下表：

n	0	1	2
a_n	$2^{M-1}RS-1$	1	$2^{M-m+2}S-2$
P_n	0	$2^M RS-2$	$2^M RS-2^{m-1}R$
Q_n	1	$2^M RS-2^{m-2}R-1$	$2^{m-2}R$

n	3	4
a_n	1	$2^M RS-2$
P_n	$2^M RS-2^{m-1}R$	$2^M RS-2$
Q_n	$2^M RS-2^{m-2}R-1$	1

$1+\alpha_n$的奇异连分数展开式为

$$\theta_0=2^M RS-\frac{1}{\theta_1}=\frac{2^M RS+\sqrt{d}}{2},$$

$$\theta_1=2^{M-m+2}S-\frac{1}{\theta_0}=\frac{2^M RS+\sqrt{d}}{2^{m-1}R}.$$

例 15 $d=4^M R^2 S^2+2^{M+1}R$, R、S是正奇数，$M\geqslant 1$。$a=1$, $b=0$, $c=4^{M-1}R^2S^2+2^{M-1}R$。$\alpha=\frac{\sqrt{d}}{2}$的简单连分数展开式如下表：

n	0	1	2
a_n	$2^{M-1}RS$	$2S$	$2^M RS$
P_n	0	$2^M RS$	$2^M RS$
Q_n	1	$2^{M-1}R$	1

α_n的奇异连分数为$\{\overline{2^M RS,\ 2S}\}$。

例 16 $d=4^M R^2 S^2-2^{M+1}R$, R、S是正奇数，$SMR>1$, $M\geqslant$

1. $a=1,\ b=0,\ c=4^{M-1}R^2S^2-2^{M-1}R,\ \alpha=\frac{\sqrt{d}}{2}$.

(a) $S=1,\ MR>1$ 时，α 的简单连分数展开式如下表：

n	0	1	2
a_n	$2^{M-1}R-1$	2	2^MR-1
P_n	0	2^MR-2	2^MR-2
Q_n	1	$2^{M-1}R-1$	1

α_k 的奇异连分数为 $\{\overline{2^MR-1,\ 2}\}$.

(b) $S>1$ 时，α 的简单连分数展开式如下表：

n	0	1	2
a_n	$2^{M-1}RS-1$	1	$2S-2$
P_n	0	2^MRS-2	2^MRS-2^MR
Q_n	1	$2^MRS-2^{M-1}R-1$	$2^{M-1}R$

n	3	4
a_n	1	2^MRS-2
P_n	2^MRS-2^MR	2^MRS-2
Q_n	$2^MRS-2^{M-1}R-1$	1

$1+\alpha_k$ 的奇异连分数为

$$\theta_0=2^MRS-\frac{1}{\theta_1}=\frac{2^MRS+\sqrt{d}}{2},$$

$$\theta_1=2S-\frac{1}{\theta_0}=\frac{2^MRS+\sqrt{d}}{2^MR}.$$

例 17 $d=4^MR^2S^2+2^{M+2}R$，R、S 是正奇数，$M\geqslant1$. $a=1$, $b=0$. $c=4^{M-1}R^2S^2+2^MR,\ \alpha=\frac{\sqrt{d}}{2}$.

(a) $S=1$ 时，α 的简单连分数展开式如下表：

n	0	1	2
a_n	$2^{M-1}R$	1	2^MR
P_n	0	2^MP	2^MR
Q_n	1	2^MR	1

$1+\alpha_k$ 的奇异连分数为

$$\theta_0 = 2^M R + 2 - \frac{1}{\theta_0} = \frac{2^M R + 2 + \sqrt{d}}{2}.$$

(b) $S>1$ 时，α 的简单连分数展开式如下表：

n	0	1	2
a_n	$2^{M-1}RS$	S	$2^M RS$
P_n	0	$2^M RS$	$2^M RS$
Q_n	1	$2^M R$	1

α_k 的奇异连分数为 $\{\overline{2^M RS,\ S}\}$

例 18 $d = 4^M R^2 S^2 - 2^{M+2} R$，$R$、$S$ 是正奇数，$SRM > 2$，$M \geqslant 1$。$a = 1$，$b = 0$，$c = 4^{M-1} R^2 S^2 - 2^M R$。$\alpha = \frac{\sqrt{d}}{2}$。

(a) $S=1$ 时，α 的简单连分数展开式如下表：

n	0	1	2
a_n	$2^{M-1}R-2$	1	$2^M R-4$
P_n	0	$2^M R-4$	$2^M R-4$
Q_n	1	$2^M R-4$	1

$1+\alpha_k$ 的奇异连分数为

$$\theta_0 = 2^M R - 2 - \frac{1}{\theta_0} = \frac{2^M R - 2 + \sqrt{d}}{2}.$$

(b) $S>1$ 时，α 的简单连分数展开式如下表：

n	0	1	2
a_n	$2^{M-1}RS-1$	1	$S-2$
P_n	0	$2^M RS-2$	$2^M RS - 2^{M+1}R$
Q_n	1	$2^M RS - 2^M R - 1$	$2^M R$

n	3	4
a_n	1	$2^M RS-2$
P_n	$2^M RS - 2^{M+1}R$	$2^M RS-2$
Q_n	$2^M RS - 2^M R - 1$	1

$1+\alpha_k$ 的奇异连分数为

$$\theta_0 = 2^M RS - \frac{1}{\theta_0} = \frac{2^M RS + \sqrt{d}}{2},\quad \theta_1 = S - \frac{1}{\theta_0} = \frac{2^M RS + \sqrt{d}}{2^{M+1}R}.$$

以上我们一共给出了 18 个例子，以下说明给出这些例子的原因。

定义 1.4 非完全平方的有理整数 d，如满足 $d\equiv 0,1 \pmod 4$，则称为判别式。命 $d_0=\frac{d}{4}$ 或 d，视 $d\equiv 0$ 或 $1 \pmod 4$ 而定。如 d_0 无平方因子，则称 d 为基本判别式。

上述十八个例子是所谓的 ERD (Extended Richaud-Degert) 型的判别式，它们的 d_0 或 $4d_0=N^2\pm r$，其中 N、r 为正整数，且有 $r\mid 4N$。详细写出，即为上述 18 种情况。

§2 Pell 方程

2.1 Pell 方程的最小解

设 d 为一个非完全平方的正整数，且 $d\equiv 0$ 或 $1 \pmod 4$，即 d 是一个正的判别式，考虑不定方程

$$x^2-dy^2=4 \tag{1.76}$$

的有理整数解 (x, y)。这个方程称为 Pell 方程。

命

$$\alpha=\begin{cases}\dfrac{\sqrt{d}}{2} \\[2mm] \dfrac{1+\sqrt{d}}{2}\end{cases}, \quad b=\begin{cases}0\\1\end{cases}, \ \text{如 } d\equiv\begin{cases}0\\1\end{cases}\pmod 4,$$

以及 $a=1$，$c=\dfrac{d-b^2}{4}$，则 c 为正整数。

由 §1 可知，α 的简单连分数展开式为

$$\alpha=[a_0, \overline{a_1, \cdots, a_k}],$$

其中 $\overline{a_1, \cdots, a_k}$ 是基本周期，并用那里的记号，对 α 的第 n 个完全商

$$\alpha_n=\frac{P_n+\sqrt{d}}{2Q_n}\ (n\geqslant 0),\ \alpha_0=\alpha$$

有(用引理 1.4)

$$Q_k=1,\ Q_l\geqslant 2(1\leqslant l\leqslant k-1)。\tag{1.77}$$

这样有

$$p_{2k-1}^2-bp_{2k-1}q_{2k-1}-cq_{2k-1}^2=1,$$

即有

$$(2p_{2k-1}-bq_{2k-1})^2-dq_{2k-1}^2=4。$$

所以得到下面的引理。

引理 2.1 Pell 方程(1.76)有解。

引理 2.2 命 Pell 方程 (1.76) 的所有正整数解中，(x_0, y_0) $(x_0>0,\ y_0>0)$ 为使 $x_0+\sqrt{d}\,y_0$ 达到最小者，则 Pell 方程 (1.76) 的所有有理整数解(x, y)可由下式得出：

$$\frac{x+\sqrt{d}\,y}{2}=\pm\left(\frac{x_0+\sqrt{d}\,y_0}{2}\right)^n,\ n\in \mathbf{Z}。$$

记

$$\varepsilon_+=\frac{x_0+\sqrt{d}\,y_0}{2},\ \varepsilon_+'=\varepsilon_+^{-1}=\frac{x_0-\sqrt{d}\,y_0}{2},$$

ε_+称为 Pell 方程(1.76)的最小解或者基本解。

证明 见华罗庚著《数论导引》第十章 p.287 的定理 2。虽然那里所考虑的方程的右端是 1，不是 4。但其证明方法可以完全照搬，我们不在此详叙了。

引理 2.3 如引理 2.2 所述，我们有

$$\varepsilon_+=p_{l-1}+\frac{\sqrt{d}-b}{2}q_{l-1},$$

这里记号如上所述，特别 $\dfrac{p_{l-1}}{q_{l-1}}$ 是 α 的第 $l-1$ 个渐近分数，

$$l=\begin{cases}k, & \text{如 } k \text{ 偶;}\\ 2k, & \text{如 } k \text{ 奇。}\end{cases}$$

证明 设 x、y 为 Pell 方程(1.76)的一个正整数解。命

$$q=y,\ p=\frac{x+by}{2},$$

则 p、q 为正整数，且有

$$ap^2-bpq-cq^2=1。$$

于是由引理 1.7 即知 $\frac{p}{q}$ 为 α 的一个渐近分数。因此有一个正整数 l，使 $p=p_{l-1}$，$q=q_{l-1}$，且 $Q_l=(-1)^l$。后者用了引理 1.1 之前的定义 (1.16)。由于 $Q_l>0$，故 l 是偶数，又 $Q_l=1$，故由 (1.77) 即知 l 为 k 的倍数。再由 ε_+ 的极小性，即得引理。

附注 1 引理 2.2 可用引理 2.3 证明中的方法得出。

附注 2 引理 2.3 的证明方法也证明了

$$\varepsilon=p_{k-1}+\frac{\sqrt{d}-b}{2}q_{k-1}$$

是广义 Pell 方程

$$x^2-dy^2=\pm 4$$

的最小解(也称为基本解)，即在这一方程的正整数解 (x, y) 中，使 $\frac{x+\sqrt{d}y}{2}$ 为最小者。实际上显然有

$$\varepsilon\cdot\varepsilon'=(-1)^k,$$

这里 $\varepsilon'=p_{k-1}-\frac{\sqrt{d}+b}{2}q_{k-1}$。

同时可见有

$$\varepsilon_+=\varepsilon \text{ 或 } \varepsilon^2,\ \text{视 } k \text{ 为偶或奇而定。}$$

k 为偶数时，这个断言显然成立；k 为奇数时，应证明一下 $\varepsilon_+=\varepsilon^2$。即应证明

$$p_{2k-1}+\beta q_{2k-1}=(p_{k-1}+\beta q_{k-1})^2, \tag{1.78}$$

其中 $\beta=\frac{\sqrt{d}-b}{2}$。我们指出

$$\alpha^2=b\alpha+c,\ \beta^2=-b\beta+c. \tag{1.79}$$

由

$$\alpha=[a_0, a_1, \cdots, a_k, (\alpha-a_0)^{-1}]=\frac{p_k(\alpha-a_0)^{-1}+p_{k-1}}{q_k(\alpha-a_0)^{-1}+q_{k-1}},$$

有(用到(1.79))

$$bq_{k-1}+q_k-a_0q_{k-1}=p_{k-1},\ cq_{k-1}=p_k-a_0p_{k-1}. \tag{1.80}$$

由

$$\frac{p_{2k-1}}{q_{2k-1}}=[a_0, a_1, \cdots, a_k, a_1, \cdots, a_{k-1}]$$

$$=\left[a_0, a_1, \cdots, a_k, \frac{q_{k-1}}{p_{k-1}-a_0q_{k-1}}\right],$$

仿上可有

$$p_{2k-1}=p_{k-1}^2+cq_{k-1}^2, \quad q_{2k-1}=2p_{k-1}q_{k-1}-bq_{k-1}^2 \qquad (1.81)$$

这里还要用一下(1.80)。

由(1.81)、(1.79)即得(1.78)。即证明了 $\varepsilon_+=\varepsilon^2$，若 k 为奇数。

引理 2.4 设有理整数 a、b、c 满足 $|b|\leqslant a\leqslant c$, g.c d. $(a, b, c)=1$，且 $d=b^2+4ac$ 不是完全平方。令

$$\alpha=\frac{b+\sqrt{d}}{2a}, \quad \beta=\frac{-b+\sqrt{d}}{2a}.$$

把 α 如 §1 所述的那样展开为简单连分数，并采用那里的记号，则广义 Pell 方程

$$x^2-dy^2=\pm 4$$

的基本解(即最小解)

$$\varepsilon=p_{k-1}+\beta q_{k-1}, \qquad (1.82)$$

而 Pell 方程

$$x^2-dy^2=4$$

的基本解

$$\varepsilon_+=\begin{cases}\varepsilon, & \text{如 } k \text{ 为偶数;}\\ \varepsilon^2, & \text{如 } k \text{ 为奇数,}\end{cases} \qquad (1.83)$$

且有 $\varepsilon\varepsilon'=(-1)^k$，这里 $\frac{p_l}{q_l}$ 为 α 的简单连分数展开式

$$\alpha=[a_0, \overline{a_1, \cdots, a_k}]$$

的第 l 个渐近分数，$\overline{a_1, \cdots, a_k}$ 是基本周期，k 是基本周期的长度。

证明 首先可知当 $d=5$ 时, $a=c=1$, $b=\pm 1$，这时引理显然成立。以下总假定 $d>5$。

第一步证明 $a|q_{k-1}$：由 §1 有(用定义(1.16)及(1.37))

$$(-1)^k a=(-1)^k Q_k=ap_{k-1}^2-bp_{k-1}q_{k-1}-cq_{k-1}^2.$$

于是

$$(bp_{k-1}+cq_{k-1})q_{k-1}\equiv 0(\bmod a),\tag{1.84}$$

再由(1.19)、(1.36)、(1.15)有

$$P_k=2a_kQ_k-P_{k+1}=2a_ka-P_1=2a_ka-2a_0a+b,$$

由此结合定义 (1.17)，即有

$$(bp_{k-2}+cq_{k-2})q_{k-1}\equiv 0(\bmod a).\tag{1.85}$$

由(1.84)、(1.85)可得

$$bq_{k-1}\equiv cq_{k-1}\equiv 0(\bmod a),$$

由此及 $g.c.d\ (a,\ b,\ c)=1$，即得 $a\mid q_{k-1}$。

同理可以证明 $a\mid q_{kl-1}(l\geqslant 1)$。

命

$$x=p_{kl-1}-\frac{b-b_0}{2}\frac{q_{kl-1}}{a},\quad y=\frac{q_{kl-1}}{a},$$

其中 $b_0=1$ 或 0，视 $d\equiv 1$ 或 $0(\bmod 4)$ 而定。

再命 $\omega=\frac{b_0+\sqrt{d}}{2}$. 则 $x,\ y\in\mathbb{Z}$，且有

$$\begin{aligned}x-y\omega&=p_{kl-1}-\frac{b-b_0}{2}\frac{q_{kl-1}}{a}-\frac{q_{kl-1}}{a}\frac{b_0+\sqrt{d}}{2}\\&=p_{kl-1}-q_{kl-1}\alpha,\end{aligned}$$

从而对

$$\omega'=\frac{b_0-\sqrt{d}}{2},\ \alpha'=\frac{b-\sqrt{d}}{2a},$$

有

$$\begin{aligned}&(x-y\omega)(x-y\omega')=(p_{kl-1}-q_{kl-1}\alpha)(p_{kl-1}-q_{kl-1}\alpha')\\&=p_{kl-1}^2-\frac{b}{a}p_{kl-1}q_{kl-1}-\frac{c}{a}q_{kl-1}^2=(-1)^{kl}\frac{Q_{kl}}{a}=(-1)^{kl}.\end{aligned}$$

这样有理整数

$$X=2x-b_0y,\ Y=y$$

满足广义的 Pell 方程

$$X^2-dY^2=\pm 4,$$

且

$$\frac{X-\sqrt{d}\,Y}{2}=x-\omega y=p_{kl-1}-q_{kl-1}\alpha,$$

又不难由

$$\frac{p_{kl-1}}{q_{kl-1}}=[a_0,\ a_1,\ \cdots,\ a_{kl-1}]>a_0,$$

可证 $X,\ Y>0$。

反之，设 $X,\ Y\in\mathbb{Z}$ 满足

$$X^2-dY^2=\pm 4.$$

命

$$x=\frac{X+b_0Y}{2},\ y=Y,$$

则 $x,\ y\in\mathbb{Z}$，且 $X,\ Y>0$ 时，$x,\ y>0$。

再命

$$p=x+\frac{b-b_0}{2}y,\ q=ay,$$

则 $p,\ q\in\mathbb{Z}$。我们来证明 $X,\ Y>0$ 时，有 $p,\ q>0$。

$b\geqslant 0$ 时，这一断言显然成立。在 $b<0$ 时，由

$$4acY^2\pm 4\geqslant 0,$$

可知 $dY^2\pm 4\geqslant b^2Y^2$，因此

$$X=\sqrt{dY^2\pm 4}\geqslant -bY,\ 故\ p=\frac{X+bY}{2}\geqslant 0.$$

如有 $p=0$，则仔细考察上述推理过程，即知必是 $a=c=1$，$b=-1$，从而 $d=5$ 的情况，这已在引理证明的开头讨论过了。于是有 $p>0$，$q>0$ 是显然的。

又由

$$p-q\alpha=x-\omega y=\frac{X-\sqrt{d}\,Y}{2},\ p-q\alpha'=\frac{X+\sqrt{d}\,Y}{2},$$

可得

$$ap^2-bpq-cq^2=a(p-q\alpha)(p-q\alpha')=a\frac{X^2-dY^2}{4}=\pm a. \tag{1.86}$$

我们再来证明 $g.c.d(p,\ q)=1$。

设素数$u|p$, q.由(1.86)，有$u^2|a$.令正整数n，使得$u^{n+1}\|a$.由$q=ay$，可得$u^{n+1}|q$。又由n的定义有$u^{n-1}\|\frac{a}{u^2}$。但由(1.86)，有

$$\pm\frac{a}{u^2}=a\left(\frac{p}{u}\right)^2-b\left(\frac{p}{u}\right)\left(\frac{q}{u}\right)-c\left(\frac{q}{u}\right)^2,$$

从而$u^n\left|\frac{a}{u^2}\right.$，这与$u^{n-1}\left\|\frac{a}{u^2}\right.$矛盾，这就证明了$g.c.d.(p,\ q)=1$。又由引理的假设可知$|\pm a|<\frac{\sqrt{d}}{2}$。这样，由引理1.7，即知$\frac{p}{q}$是$\alpha$的一个渐近分数。即有

$$p=p_{t-1},\ q=q_{t-1},\ t\geqslant 1. \tag{1.87}$$

由(1.86)、(1.87)及(1.16)，有

$$Q_t=a. \tag{1.88}$$

以下来证明$k|t$：由$q_{t-1}=q=ay$，可知$a|q_{t-1}$。故$t\geqslant 2$时，由(1.17)有$(-1)^{t-1}P_t=2ap_{t-1}p_{t-2}-b(p_{t-1}q_{t-2}+p_{t-2}q_{t-1})-2cq_{t-1}\cdot q_{t-2}\equiv(-1)^{t-1}b\pmod{2a}$，其中还用到$p_{t-1}q_{t-2}-p_{t-2}q_{t-1}=(-1)^t$。于是有

$$P_t\equiv b\pmod{2a}. \tag{1.89}$$

再由(1.19)、(1.88)和(1.89)，有

$$P_{t+1}\equiv -b\pmod{2a}. \tag{1.90}$$

而当$t=1$时，由$1=q_0=q=ay$，即知$a=1$。所以(1.90)总是成立的。这样，由(1.90)有

$$P_{t+1}=2as-b,\ s\in\mathbf{Z}. \tag{1.91}$$

由(1.31)有

$$\sqrt{d}<2Q_t+P_{t+1}=2(s+1)a-b,$$

其中还用到(1.88)与(1.91)，因此得到$s\geqslant a_0$.我们要证明$s=a_0$。用反证法：如有$s\geqslant a_0+1$，则由(1.91)有

$$P_{t+1}\geqslant 2a_0a-b+2a>2a\left(\frac{b+\sqrt{d}}{2a}-1\right)-b+2a=\sqrt{d},$$

这与$P_{t+1}<\sqrt{d}$（见(1.23)）矛盾。所以必有$s=a_0$。从而由

(1.91) 与(1.15)有

$$P_{t+1}=2a_0a-b=P_1. \tag{1.92}$$

由(1.88)、(1.92)，有

$$Q_{t+1}=\frac{d-P_{t+1}^2}{4Q_t}=\frac{d-P_1^2}{4Q_0}=Q_1. \tag{1.93}$$

由(1.92)与(1.93)即有 $k|t$。

综上所述，我们证明了广义 Pell 方程

$$X^2-dY^2=\pm 4$$

的正整数解(X, Y)具有下述形式：

$$\frac{X-\sqrt{d}Y}{2}=p_{tk-1}-q_{tk-1}\alpha,\ t\geqslant 1,$$

也即

$$\frac{X+\sqrt{d}Y}{2}=p_{tk-1}+q_{tk-1}\beta,\ t\geqslant 1,$$

其中

$$\beta=\frac{\sqrt{d}-b}{2a}.$$

由 $\beta>0$，即知，基本解

$$\varepsilon=p_{k-1}+q_{k-1}\beta.$$

易知有

$$\varepsilon\varepsilon'=\frac{1}{a}(p_{k-1}^2-bp_{k-1}q_{k-1}-cq_{k-1}^2)=(-1)^k\frac{Q_k}{a}=(-1)^k.$$

由于我们已对任一个正整数 t 均已证明 $a|q_{tk-1}$。这样可以用引理 2.3 之后附注 2 的办法以及归纳法，不难证明

$$p_{tk-1}+\beta q_{tk-1}=\varepsilon^t.$$

从而可以得出关于 ε_+ 的结论。引理证毕。

附注 命

$$\varepsilon=\frac{x_0+\sqrt{d}y_0}{2}$$

是广义 Pell 方程

$$x^2-dy^2=\pm 4 \tag{1.94}$$

的基本解，则(1.94)的所有有理整数解(x, y)如下：

$$\frac{x+\sqrt{d}\,y}{2}=\pm\varepsilon^n,\ n\in\mathbf{Z}.$$

引理 2.5 如引理2.4所设，则有

$$\varepsilon=\prod_{l=1}^{k}\alpha_l,$$

其中 α_l 是 α 的第 l 个完全商。

证明 命 $p_{-1}=1$, $p_{-2}=0$. 我们首先来证明下列断言：

$$\alpha_0\alpha_1\cdots\alpha_m=p_{m-1}\alpha_m+p_{m-2}(m\geqslant 0). \tag{1.95}$$

我们用归纳法来证明 (1.95)。$m=0$ 时，(1.95) 显然成立，设(1.95)于m时成立。由定义，(1.19)与(1.18)可有

$$\begin{aligned}p_{m-1}\alpha_m+p_{m-2}&=p_{m-1}\frac{P_m+\sqrt{d}}{2Q_m}+p_{m-2}\\&=p_{m-2}+\frac{2a_mQ_m-P_{m+1}+\sqrt{d}}{2Q_m}\,p_{m-1}\\&=p_{m-2}+a_mp_{m-1}+\frac{\sqrt{d}-P_{m+1}}{2Q_m}\,p_{m-1}\\&=p_m+\frac{2Q_{m+1}}{\sqrt{d}+P_{m+1}}\,p_{m-1}=p_m+\frac{p_{m-1}}{\alpha_{m+1}},\end{aligned}$$

由此及归纳假设，有

$$\alpha_0\alpha_1\cdots\alpha_m\alpha_{m+1}=(p_{m-1}\alpha_m+p_{m-2})\alpha_{m+1}=p_m\alpha_{m+1}+p_{m-1}.$$

归纳法完成。所以(1.95)成立。

于是由(1.95)可得

$$\alpha_0\alpha_1\cdots\alpha_k=p_{k-1}\alpha_k+p_{k-2}=p_{k-1}(\alpha_k-a_0+\alpha_0)+p_{k-2}, \tag{1.96}$$

其中用到

$$\begin{aligned}\alpha_k&=\frac{P_k+\sqrt{d}}{2Q_k}=\frac{2a_kQ_k-P_{k+1}+\sqrt{d}}{2Q_k}\\&=a_k+\frac{\sqrt{d}-P_1}{2Q_0}=a_k+\frac{\sqrt{d}-2a_0a+b}{2a}=a_k-a_0+\alpha_0.\end{aligned}$$

这样，由(1.96)有

$$\begin{aligned}\alpha_0\alpha_1\cdots\alpha_k&=p_k-a_0p_{k-1}+p_{k-1}\alpha_0=p_k-a_0p_{k-1}+\alpha_0\varepsilon-\alpha_0\beta q_{k-1}\\&=p_k-a_0p_{k-1}-\frac{c}{a}q_{k-1}+\alpha_0\varepsilon=\alpha_0\varepsilon,\end{aligned} \tag{1.97}$$

其中用到 $\varepsilon = p_{k-1} + \beta q_{k-1}$，$\alpha_0\beta = \alpha\beta = \dfrac{c}{a}$，以及

$$p_k - a_0 p_{k-1} = \frac{c}{a} q_{k-1},$$

这后一个等式，由于 $a \mid q_{k-1}$，故可用与引理 2.3 之后附注 2 相同的方法证明之。从而由(1.97)即得引理。

用同样的办法，可以证明下面的引理 2.6 及引理 2.7。

引理 2.6　如引理 2.4 所设，并记 $\tilde{\alpha}_n$ 为 α 的半单连分数展开式的第 n 个完全商。设 $\tilde{\alpha}_1, \cdots, \tilde{\alpha}_{k'}$ 为取自一个基本周期(假定循环节从 $n=0$ 开始)。则有

$$\prod_{n=1}^{k'} \tilde{\alpha}_n = \varepsilon_+.$$

引理 2.7　如引理 1.11 所设。并设 $\hat{\alpha}_n$ 为 θ（它相似于 α）的奇异连分数展开式的第 n 个完全商。设 $\hat{\alpha}_1, \cdots, \hat{\alpha}_k$ 为取自一个基本周期(假定循环节从 $n=0$ 开始)。则有

$$\prod_{n=1}^{k} \hat{\alpha}_n = \varepsilon.$$

下面，我们给出一些例子。由第二章的 genus 理论可知，类数为 1 的实二次域，仅可能域的判别式(二次域的判别式均为基本判别式) $d = 4d_0$ 或 d_0 为下列情形之一者：

$d_0 =$ 素数 $p \equiv 1 \pmod 4$；$d_0 = 2$；$d_0 =$ 素数 $q \equiv 3 \pmod 4$；

$d_0 = 2q$，素数 $q \equiv 3 \pmod 4$；$d_0 = q_1 q_2$，$q_1 \neq q_2$，$q_1 \equiv q_2 \equiv 3 \pmod 4$ 均为素数。

因此我们最感兴趣的 d 是既具有上述形式，又是所谓 ERD 型的判别式。根据这些要求，我们给出下面的例子。

例 1　$d = 4N^2 + 1$，$N \geqslant 2$。$\alpha = \dfrac{1+\sqrt{d}}{2}$ 的简单连分数如下：

n	0	1	2	3
a_n	N	1	1	$2N-1$
P_n	1	$2N-1$	1	$2N-1$
Q_n	1	N	N	1

$\varepsilon = 2N + \sqrt{d}$，$\varepsilon_+ = \varepsilon^2$。

例 2 $d=(2N+1)^2+4,\ N\geqslant 0,\ \alpha=\frac{1+\sqrt{d}}{2}$ 的简单连分数如下：

n	0	1
a_n	$N+1$	$2N+1$
P_n	1	$2N+1$
Q_n	1	1

$\varepsilon=\frac{2N+1+\sqrt{d}}{2},\ \varepsilon_+=\varepsilon^2$.

例 3 $d=4(2N+1)^2-8,\ N\geqslant 1.\ \alpha=\frac{\sqrt{d}}{2}$ 的简单连分数如下：

n	0	1	2	3	4
a_n	$2N$	1	$2N-1$	1	$4N$
P_n	0	$4N$	$4N-2$	$4N-2$	$4N$
Q_n	1	$4N-1$	2	$4N-1$	1

$\varepsilon_+=\varepsilon=4N^2+4N+(2N+1)\sqrt{4N^2+4N-1}$.

例 4 $d=16N^2-8$, N 为正偶数, $\alpha=\frac{\sqrt{d}}{2}$ 的简单连分数如下：

n	0	1	2	3	4
a_n	$2N-1$	1	$2N-2$	1	$4N-2$
P_n	0	$4N-2$	$4N-4$	$4N-4$	$4N-2$
Q_n	1	$4N-3$	2	$4N-3$	1

$\varepsilon_+=\varepsilon=4N^2-1+2N\sqrt{4N^2-2}$.

例 5 $d=4(2N+1)^2+8,\ N\geqslant 0,\ \alpha=\frac{\sqrt{d}}{2}$ 的简单连分数如下：

n	0	1	2
a_n	$2N+1$	$2N+1$	$4N+2$
P_n	0	$4N+2$	$4N+2$
Q_n	1	2	1

$\varepsilon_+ = \varepsilon = 4N^2 + 4N + 2 + (2N+1)\sqrt{4N^2+4N+3}$。

例 6 $d = 16(2N+1)^2 + 8$, $N \geqslant 0$, $\alpha = \frac{\sqrt{d}}{2}$ 的简单连分数如下：

n	0	1	2
a_n	$2(2N+1)$	$2(2N+1)$	$4(2N+1)$
P_n	0	$4(2N+1)$	$4(2N+1)$
Q_n	1	2	1

$\varepsilon_+ = \varepsilon = 16N^2 + 16N + 5 + 2(2N+1)\sqrt{16N^2+16N+6}$。

例 7 $d = (2N+1)^2 - 4$, N 为正偶数, $\alpha = \frac{1+\sqrt{d}}{2}$ 的简单连分数如下：

n	0	1	2
a_n	N	1	$2N-1$
P_n	1	$2N-1$	$2N-1$
Q_n	1	$2N-1$	1

$\varepsilon_+ = \varepsilon = \frac{2N+1+\sqrt{d}}{2}$。

例 8 $d = 4N^2 - R$, R 是正奇数, $N = MR$, M 是正整数, 且 $R \equiv 3 \pmod 4$。$\alpha = \frac{1+\sqrt{d}}{2}$ 的简单连分数如下：

n	0	1	2	3	4
a_n	N	2	$2M-1$	2	$2N-1$
P_n	1	$2N-1$	$2N-R$	$2N-R$	$2N-1$
Q_n	1	$N-\frac{R+1}{4}$	R	$N-\frac{R+1}{4}$	1

$\varepsilon_+ = \varepsilon = 8NM - 1 + 4M\sqrt{d}$。

例 9 $d = (2N+1)^2 + 4R$, 正奇数 $R \equiv 3 \pmod 4$, $2N+1 = MR$, M 为正整数。$\alpha = \frac{1+\sqrt{d}}{2}$ 的简单连分数展开式如下：

n	0	1	2
a_n	$N+1$	M	$2N+1$

P_n	1	$2N+1$	$2N+1$
Q_n	1	R	1

$$\varepsilon_+=\varepsilon=\frac{(2N+1)M+2+M\sqrt{d}}{2}.$$

例 10 $d=(2N+1)^2-4R$，正奇数 $R\equiv 3 \pmod 4)$，$2N+1=MR$，正整数 $M>1$。$\alpha=\frac{1+\sqrt{d}}{2}$ 的简单连分数展开式如下：

n	0	1	2	3	4
a_n	N	1	$M-2$	1	$2N-1$
P_n	1	$2N-1$	$2N+1-2R$	$2N+1-2R$	$2N-1$
Q_n	1	$2N-R$	R	$2N-R$	1

$$\varepsilon_+=\varepsilon=\frac{(2N+1)M-2+M\sqrt{d}}{2}.$$

2.2 $ax^2-bxy-cy^2=Q$ 的解

本小节的内容是经典的，可见之于华罗庚著《数论导引》第十一章。但为引用方便起见，把结果扼要的列举一下。

设有理整数 a, b, c 满足 $g.c.d(a, b, c)=1$，且 $d=b^2+4ac$ 不是完全平方，所以 $ac\neq 0$。设 Q 为一个有理正整数。我们来求不定方程

$$ax^2-bxy-cy^2=Q \tag{1.98}$$

的有理整数解 (x, y)。$g.c.d.(x, y)=1$ 的解，称为既约解。

引理 2.8 设 (x, y) 为 (1.98) 的一个既约解，则可唯一地决定二个整数 r, s 使

$$xs-yr=1,\ l=(2ax-by)r-(bx+2cy)s$$

满足

$$l^2\equiv d \pmod{2Q},\ 0\leqslant l<2Q.$$

引理 2.9 若 (x_1, y_1) 与 (x_2, y_2) 为(1.98) 的对应于同一个 l 的二个既约解，则有

$$x_1+\frac{\sqrt{d}-b}{2a}y_1=\left(x_2+\frac{\sqrt{d}-b}{2a}y_2\right)\frac{t+u\sqrt{d}}{2},$$

其中 $t, u\in\mathbb{Z}$ 是不定方程

$$t^2-du^2=4$$

的解。

反之，若 (x_2, y_2) 是(1.98)的一个既约解，则如上决定的 (x_1, y_1) 也是(1.98)的一个既约解，且有相同的 l。

证明　事实上

$$t=\frac{(2ax_1-by_1)(2ax_2-by_2)-dy_1y_2}{2aQ},\quad u=-\frac{(x_1y_2-x_2y_1)}{Q}$$

即合要求。

引理 2.10　当 $d<0$ 时，命

$$w=\begin{cases}2, & 如\ d<-4;\\ 4, & 如\ d=-4;\\ 6, & 如\ d=-3.\end{cases}$$

则恰有 w 个既约解对应于同一个 l。

定义 2.1　设 $d>0$。如(1.98)的一个解 (x, y) 满足

$$2ax+(b-\sqrt{d})y>0,$$

$$1\leqslant\left|\frac{2ax+(\sqrt{d}+b)y}{2ax-(\sqrt{d}-b)y}\right|<\varepsilon_+^2,$$

这里 ε_+ 是 Pell 方程

$$t^2-du^2=4$$

的最小解。则称解 (x, y) 为(1.98)的原解。

引理 2.11　设 $d>0$，如果对应于同一个 l 有既约原解，则只有唯一的既约原解。

定义 2.2　对 $d>0$，令 $w=1$。

定义 2.3　(原解定义的推广) $d>0$ 时，原解定义照旧；而 $d<0$ 时，凡解均称为原解。

于是引理 2.10 与引理 2.11 可以合并为下面的引理。

引理 2.12　对应于同一个 l，如有既约原解，则正好有 w 个既约原解。

2.3 二次同余方程的解数

在本小节内容中，我们讨论二次同余方程

$$x^2 \equiv D \pmod n$$

的解数，这里 D 与 n 均为给定的正整数，命

$$f_D(n) = \sum_{\substack{x (\bmod n) \\ x^2 \equiv D (\bmod n)}} 1.$$

引理 2.13 $f_D(n)$ 是 n 的积性函数，并且

$$f_D(n) = F_D(n) \sum_{1 \leqslant m | n} g_D(n),$$

其中 $F_D(n)$ 为 n 的积性函数：

$$F_D(n) = \prod_{p^t \| (D, n)} p^{\left[\frac{t}{2}\right]},$$

这里 p 表素数，t 表非负整数，(D, n) 表 D 与 n 的最大公约数，[ ] 表整数部分；$g_D(n)$ 也是 n 的积性函数，可如下决定之：命 $D = D_p \cdot p^{m_p}$，$p \nmid D_p$，p 表素数，m_p 是非负整数。命

$$\varepsilon_p = \begin{cases} 1, & \text{当 } p > 2 \text{；或 } p = 2,\ m_2 \text{ 为奇数时；} \\ 2, & \text{当 } p = 2,\ m_2 \text{ 偶数，而 } D_2 \equiv 3 \pmod 4 \text{ 时；} \\ 3, & \text{当 } p = 2,\ m_2 \text{ 偶数，而 } D_2 \equiv 1 \pmod 4 \text{ 时，} \end{cases}$$

及

$$\delta_p = \begin{cases} -1, & \text{当 } p > 2,\ m_p \text{ 奇数；或 } p = 2,\ m_2 \text{ 奇数；} \\ & \quad \text{或 } p = 2,\ m_2 \text{ 偶数，而 } D_2 \equiv 3 \pmod 4 \text{ 时；} \\ -2, & \text{当 } p = 2,\ m_2 \text{ 偶数，而 } D_2 \equiv 5 \pmod 8 \text{ 时；} \\ 2, & \text{当 } p = 2,\ m_2 \text{ 偶数，而 } D_2 \equiv 1 \pmod 8 \text{ 时；} \\ \left(\dfrac{D_p}{p}\right), & \text{当 } p > 2,\ m_p \text{ 偶数时。} \end{cases}$$

这里 $\left(\dfrac{*}{p}\right)$ 是 Legendre 符号，对素数幂 $p^l (l \geqslant 1)$ 有

$$g_D(p^l) = \begin{cases} 1, & \text{当 } p = 2,\ m_2 \text{ 偶数，} D_2 \equiv 1 \pmod 4 \text{，且 } l = m_2 + 2 \text{；} \\ \delta_p, & \text{当 } l = m_p + \varepsilon_p \text{；} \\ 0, & \text{其他情形。} \end{cases}$$

证明 记

$$H(n)=\sum_{1\le t|n}\mu(t)\frac{f_D\left(\frac{n}{t}\right)}{F_D\left(\frac{n}{t}\right)},$$

其中$\mu(*)$是 μöbius 函数。

易见 $f_D(n)$ 为n的积性函数，从而 $H(n)$也为n的积性函数，且有

$$H(p^l)=\frac{f_D(p^l)}{F_D(p^l)}-\frac{f_D(p^{l-1})}{F_D(p^{l-1})},\ l\geqslant 1.$$

以下简记$m=m_p$, $\varepsilon=\varepsilon_p$.

(1) 当 $p>2$ 时，$\varepsilon=1$。在$1\leqslant l<m+\varepsilon=m+1$ 时，

$$H(p^l)=f_D(p^l)p^{-\left[\frac{l}{2}\right]}-f_D(p^{l-1})p^{-\left[\frac{l-1}{2}\right]},$$

但对 $0\leqslant t\leqslant m$ 时，有

$$f_D(p^t)=p^{\left[\frac{t}{2}\right]},$$

故得

$$H(p^l)=0=g_D(p^l),\ 如\ p>2,\ l<m_p+\varepsilon_p;$$

(2) 当 $p>2$, $l>m+\varepsilon=m+1$ 时，

$$H(p^l)=(f_D(p^l)-f_D(p^{l-1}))p^{-\left[\frac{m}{2}\right]};$$

又在这时有

$$f_D(p^l)=f_D(p^{l-1}),$$

这是因为m奇时两者都是零，而m偶时，可由华罗庚著的《数论导引》定理 2.9.3 得出两者仍然相同；因此有

$$H(p^l)=0=g_D(p^l),\ 如\ p>2,\ l>m_p+\varepsilon_p;$$

(3) 当 $p>2$, $l+\varepsilon=m+1$ 时，

$$H(p^l)=(f_D(p^{m+1})-f_D(p^m))p^{-\left[\frac{m}{2}\right]};$$

容易验证，当m为奇数时，

$$f_D(p^{m+1})=0,\ f_D(p^m)=p^{\left[\frac{m}{2}\right]},$$

因此有

$$H(p^l)=-1=g_D(p^l),\ 如\ p>2,\ l=m_p+\varepsilon_p,\ 且\ m_p\ 奇;$$

也容易验证，当 m 为偶数时，

$$f_D(p^{m+1})=p^{\left[\frac{m}{2}\right]}\left(1+\left(\frac{D_p}{p}\right)\right),\ f_D(p^m)=p^{\left[\frac{m}{2}\right]},$$

因此有

$$H(p^l)=\left(\frac{D_p}{p}\right)=g_D(p^l),\ 如\ p>2,\ l=m_p+\varepsilon_p,\ 且\ m_p\ 偶;$$

(4) 当 $p=2$, m 奇数时，$\varepsilon=1$, 这时与(1)、(2), (3)一样可得 $H(p^l)=g_D(p^l)$;

(5) 当 $p=2$, m 为偶数且 $D_p\equiv 3(\mathrm{mod} 4)$时，$\varepsilon=2$。当 $1\leqslant l\neq m+\varepsilon$ 时，与(1), (2)一样可得 $H(p^l)=0=g(p^l)$。而当 $l=m+\varepsilon=m+2$ 时，

$$H(p^l)=(f_D(2^{m+2})-f_D(2^{m+1}))2^{-\frac{m}{2}},$$

而此时有

$$f_D(2^{m+2})=0,\ f_D(2^{m+1})=2^{\frac{m}{2}},$$

故可得

$$H(p^l)=-1=g_D(p^l);$$

(6) 当 $p=2$, m 为偶数，且 $D_p\equiv 1(\mathrm{mod}\ 4)$ 时，$\varepsilon=3$。

当 $1\leqslant l<m+\varepsilon-1=m+2$ 时，同上一样可得

$$H(p^l)=0=g_D(p^l);$$

又有 $H(p^{m+2})=1=g_D(p^{m+2})$ 以及

$$H(p^{m+3})=\left\{\begin{array}{l}2,\ 当\ D_p\equiv 1(\mathrm{mod}\ 8)\\ -2,\ 当\ D_p\equiv 5(\mathrm{mod}\ 8)\end{array}\right\}=g_D(p^{m+3})$$

和 $l\geqslant m+4$ 时有 $H(p^l)=0=g_D(p^l)$，这些都容易验证。

总结(1)—(6)，即得出 $H(n)=g_D(n)$。引理证毕。

附注 引理 2.13 也可改述为下述形式：

对素数幂 p^m，有

$$\left\{\begin{array}{l}p^{\left[\frac{m}{2}\right]},\ 如\ m\leqslant m_p;\\ p^{\frac{m_p}{2}},\ 如\ m=m_p+1,\ 2|m_p,\ 且\ p=2;\\ 2p^{\frac{m_p}{2}},\ 如\ m\geqslant m_p+1,\ 2|m_p,\ p>2,\ 且\ \left(\frac{D_p}{p}\right)=1;\end{array}\right.$$

$$f_D(p^m)=\begin{cases} \text{或}\ m=m_p+2,\ 2|m_p,\ p=2,\ \text{且}\ D_p\equiv 1(\bmod 4); \\ 4p^{\frac{m_p}{2}},\ \text{如}\ m\geqslant m_p+3,\ 2|m_p,\ p=2,\ \text{且}\ D_p\equiv 1 \\ \qquad (\bmod 8); \\ 0,\ \text{其他情形。} \end{cases}$$

这可由引理 2.13 通过计算得到。

2.4 实二次无理数连分数展开式周期的长度

本小节致力于证明下面的定理 2.1.

定理 2.1 设有理整数 a, b, c 满足 $|b|\leqslant a\leqslant c$, 且 $d=b^2+4ac$ 不是完全平方。再设 $\alpha=(b+\sqrt{d})/2a$ 的简单连分数为

$$\alpha=[a_0,\ \overline{a_1,\ \cdots,\ a_k}],$$

其中 $\overline{a_1,\ \cdots,\ a_k}$ 为基本周期。$p(\alpha)=k$ 称为 α 的简单连分数展开式周期的长度,简称为 α 的长度,则我们有

$$p(\alpha)=O(\sqrt{d}\log d),$$

这里 O–所含的常数是可以有效计算的绝对正常数。

证明 令 α 的第 n 个完全商为

$$\alpha_n=\frac{P_n+\sqrt{d}}{2Q_n}\ (n\geqslant 0).$$

则由引理 1.1 与引理 1.2 知有

$$d=P_n^2+4Q_nQ_{n-1}\ (n\geqslant 1),\ 1\leqslant P_n<\sqrt{d}\ (n\geqslant 1),$$

$$1\leqslant Q_n<\sqrt{d}\ (n\geqslant 0),$$

$$\sqrt{d}-P_n<2Q_n<\sqrt{d}+P_n(n\geqslant 1).$$

由此即知有

$$p(\alpha)=k\leqslant \sum_{\substack{1\leqslant n<\sqrt{d}\\ x^2\equiv d\,(\bmod 4n)\\ |2n-\sqrt{d}|<x<\sqrt{d}}} 1=\sum_{\substack{1\leqslant n<\frac{\sqrt{d}}{2}\\ x^2\equiv d\,(\bmod 4n)\\ [\sqrt{d}]-2n<x\leqslant[\sqrt{d}]}} 1+$$

$$\sum_{\substack{\frac{\sqrt{d}}{2}<n<\sqrt{d} \\ x^2\equiv d(\mathrm{mod}\,4n) \\ 2n-[\sqrt{d}]\leqslant x\leqslant[\sqrt{d}]}} 1, \tag{1.99}$$

在前一个和中，x 在一个 $\mathrm{mod}\ 2n$ 的完全剩余组中变化，又当 x 满足 $x^2\equiv d(\mathrm{mod}\ 4n)$ 时，$y=x+2nt(t\in\mathbb{Z})$ 也满足 $y^2\equiv d(\mathrm{mod}\ 4n)$，因此第一个和是

$$\sum_{\substack{1\leqslant n<\frac{\sqrt{d}}{2} \\ x^2\equiv d(\mathrm{mod}4n) \\ x(\mathrm{mod}2n)}} 1=\frac{1}{2}\sum_{\substack{1\leqslant n<\frac{\sqrt{d}}{2} \\ x^2\equiv d(\mathrm{mod}4n) \\ x(\mathrm{mod}4n)}} 1=\frac{1}{2}\sum_{1\leqslant n<\frac{\sqrt{d}}{2}} f_d(4n), \tag{1.100}$$

其中 $f_d(*)$ 如引理 2.13 所述。

(1.99) 的第二个和中，整数 x 的连续变化范围的长度是

$$2[\sqrt{d}]-2n+1<2n,$$

后一不等式是因为由

$$n>\frac{\sqrt{d}}{2}=\frac{[\sqrt{d}]+\{\sqrt{d}\}}{2}$$

可以得出

$$n\geqslant\left[\frac{[\sqrt{d}]}{2}\right]+1\geqslant\frac{[\sqrt{d}]}{2}+\frac{1}{2}>\frac{[\sqrt{d}]}{2}+\frac{1}{4},$$

这样 (1.99) 的第二个和

$$\leqslant\sum_{\substack{\frac{\sqrt{d}}{2}<n<\sqrt{d} \\ x^2\equiv d(\mathrm{mod}4n) \\ x(\mathrm{mod}2n)}} 1=\frac{1}{2}\sum_{\frac{\sqrt{d}}{2}<n<\sqrt{d}} f_d(4n). \tag{1.101}$$

总之，由 (1.99)、(1.100)、(1.101) 有

$$p(\alpha)\leqslant\frac{1}{2}\sum_{1\leqslant n<\sqrt{d}} f_d(4n)\leqslant\frac{1}{2}\sum_{1\leqslant n<4\sqrt{d}} f_d(n),$$

于是由引理 2.13 即有

$$p(\alpha)\leqslant\frac{1}{2}\sum_{1\leqslant n<4\sqrt{d}}F_d(n)\sum_{1\leqslant m\mid n}g_d(m)$$

$$=\frac{1}{2}\sum_{1\leqslant m<4\sqrt{d}}g_d(m)\sum_{1\leqslant n<\frac{4\sqrt{d}}{m}}G((d,\ mn)),\tag{1.102}$$

其中 $G(n)=\prod_{p^t\|n}p^{\left[\frac{t}{2}\right]}$, $(d,\ mn)$ 表示 d 与 mn 的最大公约数。由引理 2.13 即知,(1.102)的内和中的 m 只需取特定的,此时

$$G((d,\ mn))=G((d,\ n\prod_{p\mid m}p^{m_p+\eta_p})),$$

这里整数 $\eta_p\geqslant 1$, 于是

$$G((d,\ mn))=G(\prod_{p\mid m}p^{m_p}\cdot(d_m,\ n)),$$

其中

$$d=d_m\prod_{p\mid m}p^{m_p},\ g.c.d.(d_m,\ m)=1.$$

由 G 的积性,有

$$G((d,\ mn))=G((d_m,\ n))\prod_{p\mid m}p^{\left[\frac{m_p}{2}\right]}.\tag{1.103}$$

由(1.102)与(1.103)有

$$p(\alpha)\leqslant\frac{1}{2}\sum_{1\leqslant m<4\sqrt{d}}g_d(m)\prod_{p\mid m}p^{\left[\frac{m_p}{2}\right]}\sum_{1\leqslant n<\frac{4\sqrt{d}}{m}}G((d_m,\ n)).\tag{1.104}$$

又,对实数 $X>1$ 和正整数 u 有(μ 是 μöbius 函数)

$$\sum_{1\leqslant n\leqslant X}G(g.c.d.(u,\ n))=\sum_{\substack{1\leqslant n\leqslant X\\1\leqslant l\mid u,\ n\\g.c.d(u,\ n)=l}}G(l)$$

$$=\sum_{\substack{1\leqslant l\mid u\\1\leqslant n\leqslant\frac{lX}{u}\\g.c.d(l,\ n)=1}}G\left(\frac{u}{l}\right)$$

$$=\sum_{\substack{1\leqslant l\mid u\\ 1\leqslant n\leqslant \frac{lX}{u}}} G\left(\frac{u}{l}\right)\sum_{1\leqslant v\mid l,\, n}\mu(v)=\sum_{\substack{lv\mid u\\ 1\leqslant n\leqslant\frac{lX}{u}\\ l,\, v\geqslant 1}} G\left(\frac{u}{lv}\right)\mu(v)$$

$$=\sum_{1\leqslant l\mid u}\ \sum_{1\leqslant n\leqslant\frac{X}{l}}\ \sum_{1\leqslant v\mid l}\mu(v)G\left(\frac{l}{v}\right)=\sum_{1\leqslant l^2\mid u}\ \sum_{1\leqslant n\leqslant\frac{X}{l^2}}\varphi(l),\tag{1.105}$$

这儿 φ 是 Euler 函数，并用到

$$\sum_{1\leqslant v\mid l}\mu(v)G\left(\frac{l}{v}\right)=\begin{cases}0, & \text{如 } l \text{ 不是完全平方;}\\ \varphi(l_1), & \text{如 } l=l_1^2, \text{ 是完全平方, 且 } l_1\geqslant 1.\end{cases}$$

由(1.105)有

$$\sum_{1\leqslant n\leqslant X} G(g.c.d.(u,n))=\sum_{\substack{l^2\mid u\\ l\geqslant 1}}\varphi(l)\left[\frac{X}{l^2}\right]\leqslant X\sum_{\substack{l^2\mid u\\ l\geqslant 1}}\frac{\varphi(l)}{l^2}$$

$$=X\prod_{q^t\| u}\left(1+\frac{1}{q}-\frac{1}{q^{\left[\frac{t}{2}\right]+1}}\right)\leqslant X\prod_{q^2\mid u}\left(1+\frac{1}{q}\right),\tag{1.106}$$

这里 q 表素数，t 表非负整数。这样由(1.104)与(1.106)即有

$$p(\alpha)\leqslant 2\sqrt{d}\sum_{1\leqslant m\leqslant 4\sqrt{d}}\frac{1}{m}|g_d(m)|\cdot\prod_{p\mid m}p^{\left[\frac{m_p}{2}\right]}\prod_{q^2\mid d_m}\left(1+\frac{1}{q}\right)$$

$$\leqslant 2\sqrt{d}\prod_{p^2\mid d}\left(1+\frac{1}{p}\right)\sum_{1\leqslant m\leqslant 4\sqrt{d}}\frac{|g_d(m)|\cdot\prod_{p\mid m}p^{\left[\frac{m_p}{2}\right]}}{m}$$

于是由 $g_d(m)$ 的性质有

$$p(\alpha)\leqslant 2\sqrt{d}\prod_{p^2\mid d}\left(1+\frac{1}{p}\right)\prod_{p<4\sqrt{d}}\left(1+\frac{p^{\left[\frac{m_p}{2}\right]}}{p^{m_p+1}}\right)$$

$$\ll\sqrt{d}\prod_{p^2\mid d}\left(1+\frac{1}{p}\right)\prod_{\substack{p\leqslant 4\sqrt{d}\\ p\nmid d}}\left(1+\frac{1}{p}\right)$$

$$\ll\sqrt{d}\prod_{p\leqslant 4\sqrt{d}}\left(1+\frac{1}{p}\right)\ll\sqrt{d}\log d,$$

这里$\ll$所含常数是可以有效计算的绝对正常数。这样，完成了定理 2.1 的证明。

本 章 评 注

1．本章相当多的内容均系经典的，可参见参考文献 [35] 与 [87] 的有关内容。

2．第一节中，除引理 1.8、1.10 和引理 1.9 的个别内容外，均系引自参考文献[47]、[52]和[54]，有些则是本书中首次得到的。

3．第二节的引理 2.4 采自参考文献 [54]，引理 2.13 采自参考文献 [45]，定理 1.1 采自参考文献 [45] 与[54]，其余内容均系经典的，可参见参考文献[35] 与[87]。

第 2 章

二元二次型与二次域

本章讲述二元二次型与二次域的基本理论，主要是算术理论，包括类群、genus 理论和二元二次型与二次域的理想之间的对应关系，初步接触关于类数的 Gauss 猜想。这章的绝大部分的内容都是经典的，有些从 Gauss 时就已有了。我们在此作了比较全面和系统的介绍。

§1 二元二次型

1.1 二元二次型的分类与初等类数公式

设 d 为一个给定的判别式，即为一个给定的非完全平方的有理整数，且 $d\equiv 0$ 或 $1 \pmod 4$。再设有理整数 a, b, c 满足 $b^2-4ac=d$。显然 $ac\neq 0$。

二个变元 x, y 的二次齐次多项式

$$f=((a, b, c))=f(x, y)=ax^2+bxy+cy^2$$

称为是一个其判别式为 d 的（有理整系数的）二元二次型，并记 $d=d(f)$。今后如无特殊声明均认为型的系数是有理整数。

定义 1.1 设 $f=f(x, y)=ax^2+bxy+cy^2$ 和 $F=F(x, y)=a_1x^2+b_1xy+c_1y^2$ 是两个给定的二元二次型。如果存在有理整数 r, s, t, u 使有

$$\begin{aligned}
ru-st&=1,\\
a_1&=ar^2+brs+cs^2,\\
b_1&=2art+b(ru+st)+2csu,\\
c_1&=at^2+btu+cu^2,
\end{aligned}$$

即置

$$x=rX+tY,\ y=sX+uY$$

时，有

$$f(x,\ y)=F(X,\ Y),$$

或者用矩阵记号，有

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}\begin{pmatrix} r & t \\ s & u \end{pmatrix}=\begin{pmatrix} 2a_1 & b_1 \\ b_1 & 2c_1 \end{pmatrix},$$

那么我们称这两个二元二次型 f 和 F 为相似的，并记为

$$f\approx F,\quad 或更精密些\quad f\overset{\binom{rs}{tu}}{\approx}F;$$

否则，就称为不相似的，记为 $f\not\approx F$。

易见相似的二次型有相同的判别式。

$g.c.d.(a,\ b,\ c)=1$ 的型 $((a,\ b,\ c))$ 称为原型。

$d>0$ 的型，称为不定型，这是因为随着 $x,\ y$ 所取实值的变化，$f(x,\ y)$ 的值可正可负，也可为零。

$d<0$ 的型，称为定型，这是因为不论 $x,\ y$ 取任何实值，只要 $x,\ y$ 不同时为零，$f(x,\ y)$ 的值恒正或恒负；当恒取正值时，称为正定型，否则，称为负定型，由于负定型乘一个负号即转化为正定型，所以我们可以只讨论正定型。

引理 1.1 一个给定的二元二次型 $f(x,\ y)$ 必相似于如下的一个型

$$F(X,\ Y)=aX^2+bXY+cY^2,$$

其中有理整数 $a,\ b,\ c$ 满足

$$|b|\leqslant|a|\leqslant|c|,$$

并且

$$|a|=\min_{\substack{X,Y\in\mathbb{Z}\\(X,Y)\neq(0,0)}}|F(X,\ Y)|=\min_{\substack{x,y\in\mathbb{Z}\\(x,y)\neq(0,0)}}|f(x,\ y)|.$$

证明 显然，可参考华罗庚著《数论导引》第十二章。

易知二元二次型之间的相似关系是一种等价关系，所以可把所有二元二次型依是否相似进行分类，凡相似的分在同一类，凡不

相似的绝不在同一类。同一类的判别式相同，且同为不定型或正定型或负定型，也同为原型或非原型。

定理 1.1 判别式 d 给定的类只有有限个。

证明 本定理证明可见上述所引华罗庚所著书的第十二章。为引用方便起见，给出证明的大概。由引理 1.1 即知在每一类中有一个代表元 $((a, b, c))$，其中有理整数 a, b, c 满足

$$|b|\leqslant|a|\leqslant|c|,\ b^2-4ac=d.$$

由此即知有

$$|b|\leqslant|a|\leqslant\sqrt{\frac{|d|}{3}},\quad c=\frac{b^2-d}{4a},$$

因此 a, b, c 只有有限个可能，定理得证。

以 $H_0(d)$ 表示判别式为 d 的原型类的类数。这样以 d 为判别式的二元二次型相似类的类数

$$H(d)=\sum_{\substack{g^2\mid d\\ g\geqslant 1}} H_0\left(\frac{d}{g^2}\right).$$

定理 1.2 判别式为 d 的正定二元二次型相似类的完全代表元组可以取为

$$\left\{((a, b, c))\ \middle|\ \begin{matrix} a, b, c\in\mathbb{Z},\ b^2-4ac=d \\ -a<b\leqslant a<c \text{ 或 } 0\leqslant b\leqslant a=c\end{matrix}\right\}.$$

证明 见以上所引华罗庚所著的书的第十二章。

为给出不定型的初等类数公式，我们给出下面的定义。

定义 1.2 两个二元二次型 $f=((a,b,c))$ 与 $F=((A,B,C))$ 称为广义相似的，并记为 $f\sim F$，如果有 $f\approx F$ 或者有 $f\approx((-A, B, -C))$。

易见，当 $f\sim F$ 时，仍有 $d(f)=d(F)$。

原来的相似称为狭义相似。两个正定型如广义相似，显然一定狭义相似。但对不定型而言，就不一定了，但我们有下列的引理。

引理 1.2 设两个二元二次不定型 f 与 $F=((A, B, C))$ 满足 $f\approx((-A, B, -C))$，则它们也满足 $f\approx F$ 的充要条件是不

定方程

$$x^2-dy^2=-4$$

有有理整数解，其中 $d=d(f)=d(F)$。

证明 首先由引理1.1可知，不妨设 $f=((a,\ -b,\ -c))$，其中有理整数 $a,\ b,\ c$ 满足

$$|b|\leqslant a\leqslant c,\ g.c.d.(a,\ b,\ c)=1,\ d=b^2+4ac,$$

$$a=\min_{\substack{x,y\in\mathbb{Z}\\(x,y)\neq(0,0)}}|f(x,\ y)|\leqslant\frac{\sqrt{d}}{2}. \tag{2.1}$$

必要性的证明：由 $((a,\ -b,\ -c))\approx(A,\ B,\ C)$，容易得到

$$((a,\ b,\ -c))\approx((A,\ -B,\ C)).$$

因此有

$$((a,\ -b,\ -c))\approx((-a,\ -b,\ c)).$$

于是由定义即知，存在 $r,\ s,\ t,\ u\in\mathbb{Z}$，使

$$\begin{aligned} ru-st&=1,\\ -a&=ar^2-brs-cs^2,\\ -b&=2art-b(ru+st)-2csu,\\ c&=at^2-btu-cu^2, \end{aligned} \tag{2.2}$$

用矩阵，即有

$$\begin{pmatrix} r & s\\ t & u\end{pmatrix}\begin{pmatrix} 2a & -b\\ -b & -2c\end{pmatrix}=\begin{pmatrix} -2a & -b\\ -b & 2c\end{pmatrix}\begin{pmatrix} u & -t\\ -s & r\end{pmatrix},$$

因此有

$$at=-cs,\ a(r+u)=bs,\ c(r+u)=-bt.$$

于是有 $a\,|\,g.c.d.(cs,\ bs)=s\,g.c.d.(b,\ c)$，但 $g.c.d.(a,\ b,\ c)=1$。故

$$a\,|\,s,\ s=aR,\ R\in\mathbb{Z}.$$

以此代入(2.2)，即有

$$-1=r^2-brR-acR^2,\ -4=(2r-bR)^2-dR^2,$$

这证明了不定方程 $x^2-dy^2=-4$ 有有理整数解。

充分性的证明：由于 $x^2-dy^2=-4$ 有有理整数解，故它的基

本解 ε 满足 $\varepsilon\varepsilon'=-1$。由 (2.1) 可知 $\alpha=\frac{b+\sqrt{d}}{2a}$ 的简单连分数展开式为

$$\alpha=[a_0,\ \overline{a_1,\ \cdots,\ a_k}],$$

其中 $\overline{a_1,\cdots,a_k}$ 为基本周期，k 为基本周期长度。由 $\varepsilon\varepsilon'=-1$ 以及第一章§2.1的讨论可知 $-1=\varepsilon\varepsilon'=(-1)^k$，于是 k 为奇数。这样由第一章的记号，有

$$\begin{aligned}a=Q_k&=(-1)^k(ap_{k-1}^2-bp_{k-1}q_{k-1}-cq_{k-1}^2)\\&=-ap_{k-1}^2+bp_{k-1}q_{k-1}+cq_{k-1}^2,\end{aligned}$$

$$\begin{aligned}2(a_k-a_0)a+b=P_k&=(-1)^{k-1}(2ap_{k-1}p_{k-2}-b(p_{k-1}q_{k-2}\\&\quad+p_{k-2}q_{k-1})-2cq_{k-1}q_{k-2})\\&=2ap_{k-1}p_{k-2}-b(p_{k-1}q_{k-2}+p_{k-2}q_{k-1})\\&\quad-2cq_{k-1}q_{k-2},\end{aligned}$$

$$\begin{aligned}Q_{k-1}&=(-1)^{k-1}(ap_{k-2}^2-bp_{k-2}q_{k-2}-cq_{k-2}^2)\\&=ap_{k-2}^2-bp_{k-2}q_{k-2}-cq_{k-2}^2,\end{aligned}$$

$$p_{k-1}q_{k-2}-p_{k-2}q_{k-1}=(-1)^{k-2}=-1.$$

这四个等式说明了

$$\begin{aligned}((a,\ -b,\ -c))&\approx((-a,\ -2(a_k-a_0)a-b,\ Q_{k-1}))\\&\approx((-a,\ -b,\ c)),\end{aligned}\tag{2.3}$$

由引理的假设 $((-A,\ B,\ -C))\approx((a,\ -b,\ -c))$ 及相似的定义，可以证明

$$((A,\ -B,\ C))\approx((-a,\ b,\ c)),$$

由此可以推出

$$((A,\ B,\ C))\approx((-a,\ -b,\ c)).\tag{2.4}$$

由(2.3)、(2.4)即得 $F\approx f$。充分性也得证。

引理证毕。

容易证明二元二次型之间的广义相似也是一种等价关系，这里主要用到的事实是

$$\begin{aligned}&((a,\ b,\ c))\approx((A,\ B,\ C))\\\Longleftrightarrow&((a,\ -b,\ c))\approx((A,\ -B,\ C)).\end{aligned}$$

这已于上述引理的证明过程中应用过了，这是容易证明的。所以也可以对诸型依是否广义相似进行分类，所得的类称为广义相似类，以 $h_0(d)$ 记判别式为 d 的广义相似原型类的类数，而以 $h(d)$ 记判别式为 d 的广义相似类的类数。

由上所述及引理 1.1 和引理 1.2，可得

引理 1.3 我们有

$$h_0(d)=\begin{cases}H_0(d)\\ \frac{1}{2}H_0(d)\end{cases},\quad h(d)=\begin{cases}H(d)\\ \frac{1}{2}H(d)\end{cases},$$

$$\text{如果}\begin{cases}d<0;\ \text{或}\ d>0,\ \text{而}\ N(\varepsilon)=-1;\\ d>0,\ \text{而}\ N(\varepsilon)=1,\end{cases}$$

这里 $N(\varepsilon)=\varepsilon\varepsilon'$，而 ε 为广义 Pell 方程

$$x^2-dy^2=\pm 4$$

的基本解。

定理 1.3 对 $d>0$，我们有

$$2h_0(d)\log\varepsilon=\sum_{\substack{1\leqslant n<\sqrt{d}\\ n\equiv d\ (\mathrm{mod}\ 2)}}\left(\sum_{\substack{\frac{\sqrt{d}-n}{2}<m<\frac{\sqrt{d}+n}{2}\\ m\mid\frac{d-n^2}{4},\ g.c.d.\left(m,\,n,\,\frac{d-n^2}{4m}\right)=1}}1\right)\cdot\log\frac{\sqrt{d}+n}{\sqrt{d}-n},$$

其中 ε 为广义 Pell 方程

$$x^2-dy^2=\pm 4$$

的基本解。

证明 在第一章引理 1.9 的集合 $\mathfrak{M}$ 中取一个如下的子集

$$\mathfrak{M}_0=\left\{\omega=\frac{P+\sqrt{d}}{2Q}\in\mathfrak{M}\;\middle|\;\begin{array}{l}P,\ Q\in\mathbb{Z},\ P\equiv d\ (\mathrm{mod}\ 2),\\ \omega>2,\ 0<\omega'<1,\\ 0\neq Q\,\Big|\,\frac{P^2-d}{4}\end{array}\right\}.$$

令 $m=Q$，$n=P-2Q$。则 $\omega=\dfrac{P+\sqrt{d}}{2Q}\in\mathfrak{M}_0$ 与满足

$$0<\frac{\sqrt{d}-n}{2m}<1<\frac{\sqrt{d}+n}{2m},\ m,\ n\in\mathbb{Z},$$

$$1\leqslant n\equiv d\pmod 2,\ 1\leqslant m\left|\frac{d-n^2}{4}\right.$$

的 $\xi=\dfrac{n+\sqrt{d}}{2m}$ 一一对应。

对每一个判别式为 d 的广义相似原型类，我们可取它的一个代表 $f=((a,\ -b,\ -c))$ 如下：

$a,\ b,\ c\in\mathbb{Z},\ |b|\leqslant a\leqslant c,\ d=b^2+4ac,\ g.c.d.(a,\ b,\ c)=1$。

这样，由第一章 §1所述，我们可把 $\alpha=\dfrac{b+\sqrt{d}}{2a}$ 展开为简单连分数：

$$\alpha=[a_0,\ \overline{a_1,\ \cdots,\ a_k}],$$

其中 $\overline{a_1,\ \cdots,\ a_k}$ 为基本周期。我们仍采用那里的记号。

取 $\omega=\dfrac{P+\sqrt{d}}{2Q}\in\mathscr{M}_0$。则可知有

$$Q>0,\ P>\sqrt{d},\ \ \bar{Q}=\frac{P^2-d}{4Q}\in\mathbb{Z},\ \bar{Q}>0.$$

再设

$$g.c.d.(Q,\ P,\ \bar{Q})=1.$$

这样，二元二次原型 $F=((Q,\ P,\ \bar{Q}))$ 的判别式等于 d。

设 $F\sim f$。这可区分为两种情况。

(1) 当 $F\approx f=((a,\ -b,\ -c))$ 时，这时存在 $r,\ s,\ t,\ u\in\mathbb{Z}$，使

$$ru-st=1,$$

$$Q=ar^2-brs-cs^2,$$

$$P=2art-b(ru+st)-2csu,$$

$$\bar{Q}=at^2-btu-cu^2.$$

由此可得

$$\frac{\dfrac{-b+\sqrt{d}}{2a}u+t}{\dfrac{-b+\sqrt{d}}{2a}s+r}=\frac{P+\sqrt{d}}{2Q},$$

即有 $\omega\approx\beta=\dfrac{-b+\sqrt{d}}{2a}$，也即$\omega$与$\beta$是严格相似的。

(2) 当 $F\approx((-a,\ -b,\ c))$时，这时存在$r,\ s,\ t,\ u\in\mathbb{Z}$，使

$$ru-st=1,$$

$$Q=-ar^2-brs+cs^2,$$

$$P=-2art-b(ru+st)+2csu,$$

$$\bar{Q}=-at^2-btu+cu^2.$$

由此可得

$$\frac{\dfrac{-b+\sqrt{d}}{2a}u-t}{\dfrac{-b+\sqrt{d}}{2a}s-r}=\frac{P+\sqrt{d}}{2Q},$$

因此有 $\omega\sim\beta=\dfrac{-b+\sqrt{d}}{2a}$，但此时有$u(-r)-(-t)s=-1$，故$\omega$与$\beta$相似，但不是严格相似。

总之，在条件 $F=((Q,\ P,\ \bar{Q}))\sim f=((a,\ -b,\ -c))$时，必有 $\omega\sim\beta=\dfrac{-b+\sqrt{d}}{2a}$。把上述推导过程倒过来，可知也有逆命题，即我们有

$$((Q,\ P,\ \bar{Q}))\sim((a,\ -b,\ -c))$$
$$\Longleftrightarrow\frac{P+\sqrt{d}}{2Q}\sim\frac{-b+\sqrt{d}}{2a}.$$

再由引理1.1.9可知：当$((Q,\ P,\ \bar{Q}))\sim f=((a,\ -b,\ -c))$成立时，有

$$P-2Q=2tQ_l-P_{l+1},\quad (P-2Q)^2+4QQ_l=d,$$
$$1\leqslant t\leqslant a_l,\ 1\leqslant l\leqslant k.$$

从而条件$\omega>2,\ 0<\omega'<1$ $\left(注意\ \omega=\dfrac{P+\sqrt{d}}{2Q},\quad \omega'=\dfrac{P-\sqrt{d}}{2Q}\right)$表明了

$$2<\frac{P+\sqrt{d}}{2Q}=1+\frac{P-2Q+\sqrt{d}}{2Q}=1+\frac{2Q_l}{\sqrt{d}-(P-2Q)},$$

即

$$\frac{\sqrt{d}-2tQ_l+P_{l+1}}{2Q_l}<1,$$

即

$$a_l-t+\frac{\sqrt{d}-P_l}{2Q_l}<1,$$

再结合

$$0<\frac{\sqrt{d}-P_l}{2Q_l}<1,$$

即得

$$t=a_l,\ n=P-2Q=P_l,\ m=Q=Q_{l-1}.$$

这些论述说明了，对上述定义的 $\xi=\frac{n+\sqrt{d}}{2m}$，在条件

$$g.c.d.\left(m,\ n,\ \frac{d-n^2}{4m}\right)=1 \text{ 及 } ((Q,\ P,\ \bar{Q}))\sim f$$

成立时，是且仅是

$$\frac{\sqrt{d}+P_l}{2Q_{l-1}},\ 1\leqslant l\leqslant k.$$

注意上述论述虽然只证明了必要性，但充分性显然也是成立的。

又由第一章引理2.5可知

$$\varepsilon=\prod_{l=1}^{k}\frac{P_l+\sqrt{d}}{2Q_l}=\prod_{l=1}^{k}\frac{P_l+\sqrt{d}}{2Q_{l-1}},$$

注意后一等式的成立用了 $Q_k=Q_0=a$。

综上所述，我们得到

$$\varepsilon=\prod_{\substack{0<\frac{\sqrt{d}-n}{2m}<1<\frac{\sqrt{d}+n}{2m}\\ 1\leqslant n\equiv d\ (\mathrm{mod}\ 2)\\ 1\leqslant m\mid\frac{d-n^2}{4},\ g.c.d.\left(m,\ n,\ \frac{d-n^2}{4m}\right)=1\\ \left(\left(m,\ n+2m,\ \frac{d-n^2}{4m}-m-n\right)\right)\sim((a,\ -b,\ -c))}}\frac{n+\sqrt{d}}{2m}. \tag{2.5}$$

又容易见到，每一个判别式为 d 的原型类中都至少有一个型出现于 $\mathfrak{M}_0$ 中，这样(2.5)对判别式为 d 的所有原型类求乘积，即得

$$h_0(d)\log\varepsilon=\sum_{\substack{1\leqslant n<\sqrt{d}\\ n\equiv d\,(\mathrm{mod}\,2)}}\sum_{\substack{\frac{\sqrt{d}-n}{2}<m<\frac{\sqrt{d}+n}{2}\\ m\mid\frac{d-n^2}{4},\ g.c.d.\left(m,\,n,\,\frac{d-n^2}{4m}\right)=1}}\log\frac{n+\sqrt{d}}{2m}. \tag{2.6}$$

在(2.6)右边的求和号下，令 $m'=\dfrac{d-n^2}{4m}$，即得

$$h_0(d)\log\varepsilon=\sum_{\substack{1\leqslant n<\sqrt{d}\\ n\equiv d\,(\mathrm{mod}\,2)}}\sum_{\substack{\frac{\sqrt{d}-n}{2}<m<\frac{\sqrt{d}+n}{2}\\ m\mid\frac{d-n^2}{4},\ g.c.d.\left(m,\,n,\,\frac{d-n^2}{4m}\right)=1}}\log\frac{2m}{\sqrt{d}-n}. \tag{2.7}$$

把(2.6)与(2.7)相加，即得到所欲证明的定理。

附注 (2.6)与(2.7)也可作为类数公式。

推论 当 $d>0$ 为基本判别式时，我们有

$$2h(d)\log\varepsilon=\sum_{\substack{1\leqslant n<\sqrt{d}\\ n\equiv d\,(\mathrm{mod}\,2)}}\left(\sum_{\substack{\frac{\sqrt{d}-n}{2}<m<\frac{\sqrt{d}+n}{2}\\ m\mid\frac{d-n^2}{4}}}1\right)\log\frac{\sqrt{d}+n}{\sqrt{d}-n}$$

$$=2\sum_{\substack{1\leqslant n<\sqrt{d}\\ n\equiv d\,(\mathrm{mod}\,2)}}\sum_{\substack{\frac{\sqrt{d}-n}{2}<m<\frac{\sqrt{d}+n}{2}\\ m\mid\frac{d-n^2}{4}}}\log\frac{\sqrt{d}+n}{2m}$$

$$=2\sum_{\substack{1\leqslant n<\sqrt{d}\\ n\equiv d\,(\mathrm{mod}\,2)}}\sum_{\substack{\frac{\sqrt{d}-n}{2}<m<\frac{\sqrt{d}+n}{2}\\ m\mid\frac{d-n^2}{4}}}\log\frac{2m}{\sqrt{d}-n}.$$

证明 只需注意到 d 为基本判别式，则以 d 为判别式的型一定是原型。

1.2 二元二次型的合成

设 d 为一个给定的判别式。我们在本小节中讨论判别式为 d

的二元二次原型类的群结构，这是 Gauss 最先给出的。

定理 1.4 记判别式为 d 的二元二次原型类的全体为 $\mathscr{C}(d)$. 则 $\mathscr{C}(d)$ 是一个有限 Abel 群，其中对 $\mathscr{C}(d)$ 中的两个原型类（以 $[F]$ 表 F 所属的类）

$$[f]=[f=((a,\ b,\ c))=f(x,\ y)=ax^2+bxy+cy^2,\quad d=b^2-4ac]$$

和 $$[f']=[f'=((a',\ b',\ c'))=f'(x,\ y)=a'x^2+b'xy+c'y^2,\quad d=b'^2-4a'c'],$$

定义 $[f]$ 与 $[f']$ 的合成即群乘积为

$$[f]\circ[f']=[F]=[F=((A,\ B,\ C))=F(x,\ y)=Ax^2+Bxy+Cy^2,\ d=B^2-4AC],$$

这里 $a,\ b,\ c,\ a',\ b',\ c',\ A,\ B,\ C\in\mathbb{Z}$,

$$g.c.d.(a,\ b,\ c)=g.c.d.(a',\ b',\ c')=g.c.d.(A,\ B,\ C)=1,$$

且 $A,\ B,\ C$ 可如下决定之：

$$m=g.c.d.\left(a,\ a',\ \frac{b+b'}{2}\right),$$

$$a=a_1m,\ a'=a_1'm,\ \frac{b+b'}{2}=km,$$

$$a_1z+a_1'z'+kw=1,$$

$$A=a_1a_1',$$

$$B=b+(b'-b)a_1z-2a_1cw=b'+(b-b')a_1'z'-2a_1'c'w,$$

$$C=\frac{B^2-d}{4A},$$

以上的所有字母均表有理整数。

特别，$\mathscr{C}(d)$ 的恒等元是 $[1]=[((1,\ b_0,\ c_0))]$，这里 $c_0=\dfrac{b_0-d}{4}$，而 $b_0=0$ 或 1，视 $d\equiv 0$ 或 $1\pmod 4$ 而定。

在群的运算下，$[((a,\ b,\ c))]$ 的逆是

$$[((a,\ b,\ c))]^{-1}=[((a,\ -b,\ c))].$$

证明 首先注意，容易证明

$$b+(b'-b)a_1z-2a_1cw=b'+(b-b')a_1'z'-2a_1'c'w,$$

故B的定义是合理的，其次应证明C是整数。这是因为由

$$B^2=(b+(b'-b)a_1z-2a_1cw)(b'+(b-b')a_1'z'-2a_1'c'w)$$
$$=d+w(bb'k-dk-2bc'a_1'-2b'ca_1)$$
$$+4A\left(\left(cw+\frac{b-b'}{2}z\right)\left(c'w+\frac{b'-b}{2}z'\right)\right.$$
$$\left.+m(cz'+c'z)\right),$$

及

$$bb'k-dk-2bc'a_1-2b'ca_1$$
$$=\frac{1}{m}\left(bb'\frac{b+b'}{2}-d\frac{b+b'}{2}-2bc'a'-2b'ca\right)$$
$$=\frac{b}{2m}(b'^2-4a'c'-d)+\frac{b'}{2m}(b^2-4ac-d)=0.$$

可得

$$C=m(cz'+c'z)+\left(cw+\frac{b-b'}{2}z\right)\left(c'w+\frac{b'-b}{2}z'\right).$$

即证明了C是一个整数。

另外，为证明定理，我们需要下列的引理。

引理 设N, a, b, c为任意给定的整数，且满足

$$N\neq 0,\ g.c.d.(a,\ b,\ c)=1,$$

则存在既约整数对$(x,\ y)$，使

$$g.c.d.(ax^2+bxy+cy^2,\ N)=1.$$

证明 这个引理可见华罗庚著《数论导引》引理12.5.2.为完整起见，给出它的简短证明如下：记$F(x,\ y)=ax^2+bxy+cy^2$。对N的每一个素因子p，由于

$$g.c.d.(F(1,\ 0),\ F(0,\ 1),\ F(1,\ 1))=g.c.d.(a,\ b,\ c)=1,$$

故存在整数对$(x_p,\ y_p)$使$g.c.d(F(x_p,\ y_p),\ p)=1$，不妨设$g.c.d(x_p,\ y_p)=1$。再由中国剩余定理即得引理。

由引理，取整数Q为f原表出，即存在既约整数对$(x,\ y)$，使$f(x,\ y)=Q$，且有

$$g.c.d.(Q,\ 2daa')=1.$$

于是

$$f \approx ((Q, *, *)).$$

再由引理，取 Q' 为 f' 所表出，且

$$g.c.d.(Q', 2Qdaa') = 1. \tag{2.8}$$

于是也有

$$f' \approx ((Q', *, *)).$$

由于 $g.c.d.(Q, Q') = 1$，于是当 μ, ν 跑过所有整数时，$Q\mu - Q'\nu$ 可以表出任何整数，这样可取适当的 μ, ν 使

$$f \approx ((Q, *, *)) \overset{\binom{1\,0}{\mu\,1}}{\approx} ((Q, P, Q'T)) \overset{\text{def}}{=} g, \tag{2.9}$$

$$f' \approx ((Q', *, *)) \overset{\binom{1\,0}{\nu\,1}}{\approx} ((Q', P, QT)) \overset{\text{def}}{=} g', \tag{2.10}$$

其中 P, T 均为整数，$d = P^2 - 4QQ'T$.

令

$$G = ((QQ', P, T)), \tag{2.11}$$

则 g, g', G 均是判别式为 d 的原型。且有

$$G(X, Y) = g(x, y)g'(x', y'), \tag{2.12}$$

这里

$$X = xx' - Tyy', \quad Y = Qxy' + Q'x'y + Pyy' \tag{2.13}$$

(2.12) 可由直接计算验证。

恢复到 f, f'，即知有

$$G(X, Y) = f(x, y)f'(x', y'). \tag{2.14}$$

这里整系数双线性变换

$$X = pxx' + p_1xy' + p_2x'y + p_3yy',$$
$$Y = qxx' + q_1xy' + q_2x'y + q_3yy',$$

使下列各整数(行列式)

$$\begin{vmatrix} p & p_1 \\ q & q_1 \end{vmatrix}, \begin{vmatrix} p & p_2 \\ q & q_2 \end{vmatrix}, \begin{vmatrix} p & p_3 \\ q & q_3 \end{vmatrix}, \begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix}, \begin{vmatrix} p_1 & p_3 \\ q_1 & q_3 \end{vmatrix}, \begin{vmatrix} p_2 & p_3 \\ q_2 & q_3 \end{vmatrix}$$

的最大公约数为1。

容易看到，具有这种性质的判别式也为 d 的二元二次原型 G 所在的类只与 f 和 f' 所在的类有关，并且与 f 和 f' 的先后次序无关，即当

$$f\approx f_1,\quad f'\approx f_1'$$

时，具有上述性质的 G 与 G_1 是属于同一个类的，即有：

$$G\approx G_1.$$

这就是 Gauss 原来关于合成的定义。群运算法则的成立，也可由此而推出。因此我们只需证明定理中的 F 与现在的 G 是相似的。

由(2.9)与(2.10)，可命

$$g=((Q,\ P,\ Q'T))\overset{\left(\begin{smallmatrix} r & s\\ t & u\end{smallmatrix}\right)}{\approx}((a,\ b,\ c))=f,$$

$$g'=((Q',\ P,\ QT))\overset{\left(\begin{smallmatrix} r' & s'\\ t' & u'\end{smallmatrix}\right)}{\approx}((a',\ b',\ c'))=f'.$$

则有

$$r,\ s,\ t,\ u\in\mathbb{Z},\ ru-st=1, \tag{2.15}$$

$$a=Qr^2+Prs+Q'Ts^2, \tag{2.16}$$

$$b=2Qrt+P(ru+st)+2Q'Tsu, \tag{2.17}$$

$$c=Qt^2+Ptu+Q'Tu^2, \tag{2.18}$$

$$r',\ s',\ t',\ u'\in\mathbb{Z},\ r'u'-s't'=1, \tag{2.19}$$

$$a'=Q'r'^2+Pr's'+QTs'^2, \tag{2.20}$$

$$b'=2Q'r't'+P(r'u'+s't')+QTs'u', \tag{2.21}$$

$$c'=Q't'^2+Pt'u'+QTu'^2. \tag{2.22}$$

于是，命

$$X_0=rr'-Tss',\ Y_0=Qrs'+Q'r's+Pss'. \tag{2.23}$$

即有(用(2.12)与(2.13))

$$aa'=g(r,\ s)g'(r',\ s')=G(X_0,\ Y_0)$$
$$=QQ'X_0^2+PX_0Y_0+TY_0^2. \tag{2.24}$$

由(2.16)、(2.17)、(2.20)和(2.21)有

$$2au-bs=2Qr+Ps, \tag{2.25}$$

$$2a'u'-b's'=2Q'r'+Ps'. \tag{2.26}$$

由(2.23)、(2.25)和(2.26)可得

$$2QQ'X_0+PY_0=2aa'uu'-ab'us'-a'bu's+\frac{d+bb'}{2}ss'. \tag{2.27}$$

注意

$$\frac{d+bb'}{2}=\frac{b+b'}{2}b-2ac=\frac{b+b'}{2}b'-2a'c' \tag{2.28}$$

是一个整数。

由(2.23)、(2.25)和(2.26)还可得

$$Y_0=aus'+a'u's-\frac{b+b'}{2}ss' \tag{2.29}$$

这样由m的定义,(2.27)、(2.28)与(2.29),即得

$$m|g.c.d.(2QQ'X_0+PY_0,\ Y_0). \tag{2.30}$$

由Q的取法,及(2.8)、(2.24),即知有

$$g.c.d.(QQ',\ Y_0)=1. \tag{2.31}$$

由(2.30)及(2.31)即有

$$m|g.c.d.(2X_0,\ Y_0). \tag{2.32}$$

又由(2.23)可得

$$X_0Qs'-Y_0r'=-a's,\ X_0Q's-Y_0r=-as',$$

由此可得

$$g.c.d.(X_0,\ Y_0)|g.c.d.(a's,\ as'), \tag{2.33}$$

由Q, Q'的定义有

$$g.c.d.(a,\ Q)=g.c.d.(a',\ Q')=1,$$

再由(2.16)与(2.20)以及(2.15)与(2.19),可得

$$g.c.d.(a,\ s)=g.c.d.(a',\ s')=1,$$

从而

$$g.c.d.(a's,\ as')=g.c.d.(a,\ a')g.c.d.(s,\ s'). \tag{2.34}$$

又由(2.23)、(2.15)和(2.19)可知有

$$g.c.d.(g.c.d.(X_0,\ Y_0),\ g.c.d.(s,\ s'))=1. \tag{2.35}$$

由(2.33)—(2.35)有

$$g.c.d.(X_0,\ Y_0)|g.c.d.(a,\ a'). \tag{2.36}$$

由(2.36)、(2.27)和(2.28)可知

$$g.c.d.(X_0,\ Y_0)\left|\frac{b+b'}{2}ss'\right.. \tag{2.37}$$

不难证明

$$g.c.d.(g.c.d.(X_0,\ Y_0),\ ss')=1 \tag{2.38}$$

这可由(2.23)、(2.15)、(2.16)、(2.19)与(2.20)得出。

由(2.37)、(2.38)可得

$$g.c.d.(X_0,\ Y_0)\Big|\frac{b+b'}{2},$$

结合(2.36)，即得

$$g.c.d.(X_0,\ Y_0)\,|\,m. \tag{2.39}$$

我们来证明

$$g.c.d.(X_0,\ Y_0)=m. \tag{2.40}$$

如(2.40)不成立，则由(2.32)及(2.39)有

$$2g.c.d.(X_0,\ Y_0)=m=g.c.d.(2X_0,\ Y_0), \tag{*}$$

但这是不可能的，因为可令非负整数 e, e' 使

$$2^e\|X_0,\ 2^{e'}\|Y_0,$$

则由(*)可得 $e'\geqslant e+1$。再由*即有

$$2^{e+1}\Big|a,\ a',\ \frac{b+b'}{2},\ Y_0;\ 2^e\|X_0.$$

由此结合(2.24)即得 $2|QQ'$，这与 QQ' 为奇数的取法矛盾，这就证明了(2.40)。

命

$$X_0=Rm,\ Y_0=Sm,\ R,\ S\in\boldsymbol{Z},\ g.c.d.(R,\ S)=1. \tag{2.41}$$

则有(用(2.24))

$$QQ'R^2+PRS+TS^2=A. \tag{2.42}$$

令

$$U=uu'm-\left(cw+\frac{b-b'}{2}z\right)u's-\left(c'w+\frac{b'-b}{2}z'\right)us'$$
$$-ss'(c'z+cz'). \tag{2.43}$$

则 $U\in\boldsymbol{Z}$。由(2.27)—(2.29)可得

$$2QQ'R+PS+BS=2Auu'm+(B-b')a_1us'+(B-b)a_1'u's$$
$$+(k^2m-a_1c-a_1'c'-kB)ss',$$

这里还用到 A 的定义，再用 B 的定义，即得

$$2QQ'R+PS+BS=2Auu'm+(b-b')a_1a_1'us'z'$$

$$-2c'a_1a_1'wus'+(b'-b)a_1a_1'u'sz-2ca_1a_1'wu'ss$$
$$+ss'((k^2m-a_1c-a_1'c')(1-kw)-b'a_1zk-ba_1'z'k),$$

这里还用到 $a_1z+a_1z'+kw=1$，把这个式子再用一次，即有

$$2QQ'R+PS+BS=2A\Big(uu'm+\frac{b-b'}{2}us'z'$$
$$-c'wus'+\frac{b'-b}{2}u'sz-cwu's\Big)$$
$$+ss'(a_1z(k^2m-a_1c-a_1'c'-b'k)$$
$$+a_1'z'(k^2m-a_1c-a_1'c'-bk)).$$

再用

$$k^2m-a_1c-a_1'c'-b'k=-2a_1'c',$$
$$k^2m-a_1c-a_1'c'-bk=-2a_1c,$$

可得

$$2QQ'R+PS+BS=2AU. \tag{2.44}$$

由(2.42)与(2.44)可得

$$4QQ'A=(2QQ'R+PS)^2-dS^2=(2AU-BS)^2-dS^2$$
$$=4A^2U^2-4ABUS+4ACS^2.$$

即得

$$QQ'=AU^2-BUS+CS^2. \tag{2.45}$$

由(2.44)及(2.45)可得

$$2QQ'RU+(P-B)SU+2CS^2=2AU^2-2BUS+2CS^2=2QQ',$$

故有

$$\left(\frac{B-P}{2}U-CS\right)S=QQ'(RU-1), \tag{2.46}$$

这儿 $\frac{B-P}{2}\in\mathbb{Z}$。由(2.24)、(2.41)及 $g.c.d.(QQ',\ aa')=1$，即有

$$g.c.d.(QQ',\ S)=1. \tag{2.47}$$

所以由(2.46)与(2.47)即知，有

$$S'\in\mathbb{Z},\ RU-SS'=1, \tag{2.48}$$

$$\frac{B-P}{2}U-CS=QQ'S'. \tag{2.49}$$

由(2.49)有

$$\begin{aligned}(2QQ'S'+PU)^2&=(BU-2CS)^2\\&=dU^2+4C(AU^2-BUS+CS^2)\\&=(P^2-4QQ'T)U^2+4CQQ',\end{aligned}$$

最后一步用了 $d=P^2-4QQ'T$ 及(2.45)，由此即得

$$C=QQ'S'^2+PS'U+TU^2. \tag{2.50}$$

当 $U=0$ 时，由(2.48)有 $S'=-S=\pm1$，则由(2.44)有

$$B=-2QQ'RS-P,$$

即

$$B=2QQ'RS'+P(RU+SS')+2TSU. \tag{2.51}$$

如 $S=0$，则由(2.48)有 $U=R=\pm1$，从而由(2.49)有

$$B=2QQ'US'+P=2QQ'RS'+P(RU+SS')+2TSU,$$

即(2.51)在 $S=0$ 时，仍成立。当 $US\neq0$ 时，我们来证明(2.51)仍然成立。

由(2.45)、(2.42)与(2.50)有

$$\begin{aligned}QQ'&=AU^2-BUS+CS^2\\&=(QQ'R^2+PRS+TS^2)U^2-BUS\\&\quad+(QQ'S'^2+PS'U+TU^2)S^2\\&=QQ'(RU-SS')^2+2QQ'RUSS'\\&\quad+P(RU+SS')US+2TU^2S^2-BUS.\end{aligned}$$

用 $US\neq0$，即知此时(2.51)仍然成立。这样，由(2.42)、(2.51)、(2.50)和(2.48)即知有

$$G\overset{\left(\begin{smallmatrix}R&S\\S'&U\end{smallmatrix}\right)}{\approx}F,$$

得到所需。定理的其余的两个结论显然成立。定理证毕。

附注 由定理1.4的算法可知，a_1, a_1', $A=a_1a_1'$ 均是比较容易计算的，而 B 满足同余方程组

$$\begin{cases}B\equiv b\pmod{2|a_1|},\ B\equiv b'\pmod{2|a_1'|},\\B^2\equiv d\pmod{4|A|}.\end{cases}$$

不难证明这个同余方程 $B\pmod{2|A|}$ 有唯一解，但可见所要求的

恰好如此,所以可用求这个同余方程组的办法来算出 B。

推论 设 $f=((a,\ b,\ c))=f(x,\ y)=ax^2+bxy+cy^2$ 是一个其判别式为 d 的二元二次原型,且 $g.c.d.(a,\ d)=1$。则在 Gauss 合成下,对 $n\geqslant 2$ 有

$$[f]^n=\underbrace{[f]\circ[f]\circ\cdots\circ[f]}_{n\text{个}}=[F_n],$$

其中

$$F_n=((a_n,\ b_n,\ c_n)),$$

这里 $$a_1=a,\ b_1=b,\ c_1=c,\ a_n=a^n,$$

b_n是同余方程组

$$\begin{cases} b_n\equiv b_{n-1}(\bmod 2|a|^{n-1}) \\ b_n^2\equiv d(\bmod\ 4|a|^n) \end{cases}$$

mod $2a^n$ 的唯一解,而 c_n 由

$$b_n^2-4a_nc_n=d$$

给出。

证明 用定理1.4及附注即可证明推论在 $n=2$ 时成立,然后再对 n 用归纳法,即得所需。

例 1 设 $d=1-4q^l$, 其中 $q,\ l$ 为正整数,且 $q\geqslant 2$。易见 $f=((q,\ 1,\ q^{l-1}))$ 是以 $d<0$ 为判别式的二元二次正定原型。由推论易得

$$[f]^n=[((q^n,\ 1,\ q^{l-n}))],\ 1\leqslant n\leqslant l。$$

由此可知,对 $1\leqslant n\leqslant l$,

$$[f]^n=[1],\ \text{当且仅当}\ n=l,$$

这里 $[1]$ 是判别式为 $d=1-4q^l$ 的原型类在 Gauss 合成下所成的 Abel 群 $\mathscr{C}(d)$的恒等元,即

$$[1]=[((1,\ 1,\ q^l))]。$$

令 $h_0(d)=|\mathscr{C}(d)|$, 则由以上推理即得

$$l\,|\,h_0(d)。$$

例 2 设 $d=1+4q^{2l}$, 其中 $q,\ l$ 为正整数, 且 $q\geqslant 2$。易见 d 不是完全平方。取 $f=((q,\ 1,\ -q^{2l-1}))$。用推论, 与例1一样,

可得

$$l \mid h_0(d).$$

1.3 二元二次型的自同构群

定义 1.3 对一个给定的其判别式为 d 的二元二次型 $f=((a, b, c))=f(x, y)=ax^2+bxy+cy^2$，如果线性变换

$$U: X=rx+ty, Y=sx+uy, r, u, s, t\in\mathbb{Z},$$

使

$$f(X, Y)=f(rx+ty, sx+uy)=f(x, y),$$

则称 U 为 f 的(狭义)自同构，如 $\det\begin{pmatrix} r & s \\ t & u \end{pmatrix}=ru-st=1$；或称 U 为 f 的广义自同构，如 $\det\begin{pmatrix} r & s \\ t & u \end{pmatrix}=ru-st=-1$.

附注 在上述的定义中，可用矩阵记号：(U^T 是 U 的转置)

$$f=\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}, \quad \begin{pmatrix} X \\ Y \end{pmatrix}=U\begin{pmatrix} x \\ y \end{pmatrix}, \quad U=\begin{pmatrix} r & t \\ s & u \end{pmatrix},$$

如有 $f[U]\stackrel{\text{def}}{=}U^TfU=f$，则称 U 为 f 的(狭义)自同构，若 $\det U=1$，或称 U 为 f 的广义自同构，若 $\det U=-1$.

引理 1.4 设 $f=((a, b, c))$ 与 $F=((A, B, C))$ 为两个它们的判别式都是 d 的二元二次型，如存在 $M\in SL_2(\mathbb{Z})$ 使

$$f[M]=F,$$

则有

$$M\langle\alpha_F\rangle=\alpha_f,$$

其中

$$\alpha_F=\frac{-B+\sqrt{d}}{2A}, \quad \alpha_f=\frac{-b+\sqrt{d}}{2a}.$$

证明 直接计算可得.

引理 1.5 (a) $f=((a, b, c))$ 的全体自同构组成了一个群，称为 f 的自同构群，记为 $O_+(f)$. 设 d 为 f 的判别式，则有

$$O_+(f)=\left\{\begin{pmatrix}\frac{t-bu}{2} & -cu\\ au & \frac{t+bu}{2}\end{pmatrix}\middle| \begin{array}{l} t^2-du^2=4\\ t,\ u\in\mathbb{Z}\end{array}\right\}.$$

(b) 设 S 为 $f=((a,\ b,\ c))$ 的一个广义自同构，则

$$S^2=I,\ \det S=-1,$$

这里 I 是二阶单位方阵。

证明　(a) 由引理1.4可得。

(b) $\det S=-1$ 是已知的，由于我们已约定 $d\neq 0$，故存在非异的复方阵 P，使 $f=P^TP$，命 $S_1=PSP^{-1}$。则有 $S_1^T=S_1^{-1}$，且 $\det S_1=-1$。由此立得 $S_1^2=I$。故也有 $S^2=I$。

引理1.6　设 $f=((a,\ b,\ c))$ 是判别式为 d 的二元二次型，则有：

(a) 当 $d=-3$ 时，

$$O_+(f)=\left\{\pm I,\ \frac{\delta_1}{2}I+\frac{\delta_2}{2}\begin{pmatrix}-b & -2c\\ 2a & b\end{pmatrix},\ \delta_1,\ \delta_2=\pm 1\right\},$$

$$O_+^2(f)=\left\{I,\ -\frac{1}{2}I\pm\frac{1}{2}\begin{pmatrix}-b & -2c\\ 2a & b\end{pmatrix}\right\},$$

因此　　$|O_+(f)|=6,\ |O_+(f)/O_+^2(f)|=2;$

(b) 当 $d=-4$ 时，

$$O_+(f)=\left\{\pm I,\ \pm\frac{1}{2}\begin{pmatrix}-b & -2c\\ 2a & b\end{pmatrix}\right\},\ O_+^2(f)=\{\pm I\},$$

因此 $|O_+(f)|=4,\ |O_+(f)/O_+^2(f)|=2;$

(c) 当 $d<-4$ 时，

$$O_+(f)=\{\pm I\},\ O_+^2(f)=\{I\}$$

因此 $|O_+(f)|=2,\ |O_+(f)/O_+^2(f)|=2;$

(d) 当 $d>0$ 时，

$$O_+(f)\cong\{\pm\varepsilon_+^n|n\in\mathbb{Z}\},\ O_+^2(f)\cong\{\varepsilon_+^{2n}|n\in\mathbb{Z}\},$$

这里 ε_+ 是 Pell 方程 $x^2-dy^2=4$ 的基本解。因此

$$|O_+(f)/O_+^2(f)|=4.$$

证明　直接计算即可。

1.4　二元二次型的 genus 理论

定义 1.4　一个判别式为 d 的二元二次原型 $f=((a,b,c))$ 称为是 Ambiguous 型，如果

$$b=0 \text{ 或 } a.$$

f 所属的相似类 $[f]$ 称为 Ambiguous 类。

引理 1.7　$[f]$ 是 Ambiguous 类的充要条件是

$$[f]^2=[1], \text{ 即 } [f]^{-1}=[f].$$

证明　必要性：设 $[f]$ 是 Ambiguous 类。由定义不妨设 $[f]=[((a,b,c))]$，其中 $b=0$ 或 a。由定理 1.4 有

$$[f]^{-1}=[((a,-b,c))]=[((a,b,c))],$$

后一等式在 $b=0$ 时显然。而在 $b=a$ 时，用

$$((a,-b,c))\overset{\begin{pmatrix}1&0\\1&1\end{pmatrix}}{\approx}((a,b,c)), \quad \text{如 } a=b,$$

即可得出。这样 $[f]^{-1}=[f]$，从而 $[f]^2=[1]$。

充分性：如有 $[f]=[f]^{-1}$，设 $f=((a,b,c))$，即有

$$((a,-b,c))\approx((a,b,c)).$$

因此存在 $r,s,t,u\in\boldsymbol{Z}$，使

$$ru-st=1,$$

$$a=ar^2+brs+cs^2,$$

$$-b=2art+b(ru+st)+2csu,$$

$$c=at^2+btu+cu^2.$$

用矩阵写出，即有

$$\begin{pmatrix}r&s\\t&u\end{pmatrix}\begin{pmatrix}2a&b\\b&2c\end{pmatrix}=\begin{pmatrix}2a&-b\\-b&2c\end{pmatrix}\begin{pmatrix}u&-t\\-s&r\end{pmatrix}.$$

可得

$$r=u, \quad at+br+cs=0. \tag{2.52}$$

我们分几种情况：

(1)　如 $r=u=0$，则有 $s=-t=\pm1$，并由 (2.52) 有 $c=a$，此

时

$$f=((a,\ b,\ c))=((a,\ b,\ a))\overset{\binom{1\ 1}{0\ 1}}{\approx}((2a+b,\ 2a+b,\ a)),$$

所以$[f]$是 Ambiguous 类。

(2) 如 $r=u\neq 0$, 则有 $r^2-1=st$, 故有

$$r+1=s_1t_1,\ r-1=s_2t_2,\ s=s_1s_2,\ t=t_1t_2,$$

$$2r=s_1t_1+s_2t_2,\ s_1t_1-s_2t_2=2,\ s_1,\ s_2,\ t_1,\ t_2\in\mathbb{Z}.$$

(a) r 偶, s_1, s_2, t_1, t_2 均奇; 或 r 奇, 而 s_1 与 s_2 同奇偶, t_1 与 t_2 同奇偶。此时命

$$R=t_2,\ S=s_1,\ T=\frac{t_2-t_1}{2},\ U=\frac{s_1-s_2}{2},\ R,\ S,\ T,\ U\in\mathbb{Z},$$

则有

$$RU-ST=t_2\frac{s_1-s_2}{2}-s_1\frac{t_2-t_1}{2}=\frac{s_1t_1-s_2t_2}{2}=1,$$

$$R^2-2RT=R(R-2T)=t_2(t_2-(t_2-t_1))=t_2t_1=t,$$

$$RS-RU-ST=t_2s_1-t_2\frac{s_1-s_2}{2}-s_1\frac{t_2-t_1}{2}$$

$$=\frac{s_2t_2+s_1t_1}{2}=r,$$

$$S^2-2SU=S(S-2U)=s_1(s_1-s_1+s_2)=s_1s_2=s,$$

于是有

$$aR^2+bRS+cS^2-(2aRT+b(RU+ST)+2cSU)$$
$$=a(R^2-2RT)+b(RS-RU-ST)+c(S^2-2SU)$$
$$=at+br+cs=0,$$

最后一步用了(2.52)。从而有

$$f=((a,\ b,\ c))\overset{\binom{R\ S}{T\ U}}{\approx}((A,\ A,\ *)),$$

这证明了$[f]$为一个 Ambiguous 类。

(b) r 奇, s 与 t 均偶(如 r 奇而 s, t 中有一个为奇数, 则归结为上述的情况(a))。这时又可分为两种子情况。

ⓑ′ s_1, t_2 偶与ⓑ″ s_2, t_1 偶。分别考虑之。

ⓑ′ s_1, t_2 偶。此时命

$$R=t_1,\ S=s_2,\ T=\frac{t_2}{2},\ U=\frac{s_1}{2},\ R,\ S,\ T,\ U\in\mathbb{Z}.$$

则有

$$RU-ST=\frac{s_1t_1-s_2t_2}{2}=1,$$

$$2RT=t_1t_2=t,\ RU+ST=\frac{s_1t_1+s_2t_2}{2}=r,\ 2SU=s_1s_2=s.$$

于是用(2.52)即有

$$2aRT+b(RU+ST)+2cSU=at+br+cs=0.$$

所以有

$$f=((a,\ b,\ c))\overset{\binom{R\ S}{T\ U}}{\approx}((*,\ 0,\ *)).$$

这证明了[f]为 Ambiguous 类。

ⓑ″ s_2, t_1 偶，此时命

$$R=\frac{t_1}{2},\ S=\frac{s_2}{2},\ T=t_2,\ U=s_1,\ R,\ S,\ T,\ U\in\mathbb{Z}.$$

则有

$$RU-ST=1,\ 2RT=t,\ RU+ST=r,\ 2SU=s,$$

从而由(2.52)即有

$$2aRT+b(RU+ST)+2cSU=at+br+cs=0.$$

因此有

$$f=((a,\ b,\ c))\overset{\binom{R\ S}{T\ U}}{\approx}((*,\ 0,\ *)),$$

这也证明了[f]为 Ambiguous 类，引理证毕。

引理 1.8 在一个 Ambiguous 类中所含的 Ambiguous 型的个数为 2，如 $d<0$；或为 4，如 $d>0$。这里 d 是判别式。

证明 设 $\mathfrak{A}$ 为一个给定的 Ambiguous 类，在 $\mathfrak{A}$ 中取定一个型 F，F 的判别式是 d。

我们简述证明步骤如下：

(1) $f=((a,\ b,\ c))$ 为 Ambiguous 型的充要条件为 $R_w=\begin{pmatrix}1 & w\\ 0 & -1\end{pmatrix}$ ($w=0$ 或 1)是 f 的一个广义自同构，且当 $f=$

$((a,\ b,\ c))$为 Ambiguous 型时，$b=aw$。

这是显然的。

(2) 如$f=((a,\ b,\ c))$是$\mathscr{U}$中的一个 Ambiguous 型，则存在F的一个广义自同构S，和一个$M\in SL_2(\mathbb{Z})$，使

$$f=F[M],\ SM=MR_w,\ \ R_w=\begin{pmatrix}1 & w\\ 0 & -1\end{pmatrix},\ \ w=\frac{b}{a}=0\text{ 或 }1.$$

这由(1)及定义可得。

(3) 如S为F的一个广义自同构，则必存在一个$M\in SL_2(\mathbb{Z})$，使

$$SM=MR_w,\ R_w=\begin{pmatrix}1 & w\\ 0 & -1\end{pmatrix},\ w=0\text{ 或 }1,$$

且$F_S=F[M]=((a,\ b,\ c))$为一个 Ambiguous 型，同时$b=aw$。

这是因为由引理1.5(b) 知有$S^2=I$, $\det S=-1$。故可先取互素的整数列向量ξ，使$S\xi=\xi$，再取整数列向量η，使$(\xi,\ \eta)\in -SL_2(\mathbb{Z})$，则可知有$S(\xi,\eta)=(\xi,\ \eta)=\begin{pmatrix}1 & \lambda\\ 0 & -1\end{pmatrix}$, $\lambda\in\mathbb{Z}$。最后取$u\in\mathbb{Z}$，使$\lambda+2u=w=0$或1，则$M=(\xi,\ \eta)\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}$即为所求，其余显然。

(4) 易见在(3)的构作中，由同一个S所得的w一定相同，而M只差一个符号，从而所得的$F_S=F[M]$是唯一确定的。

(5) 设S, S_1为F的两个广义自同构，则(3)中所构作的两个 Ambiguous 型F_S与F_{S_1}相同的充要条件是存在$T\in O_+(F)$使$S_1=T^2S$。

充分性　因为TS与S一样都是F的广义自同构，所以有$S^2=I=(TS)^2=TSTS$，即$S=TST$。从而$S_1=T^2S$满足$S_1TM=TMR_w$，于是$F_{S_1}=F[TM]=F[M]=F_S$。

必要性　令$S_1M_1=M_1R_{w_1}$, $M_1\in SL_2(\mathbb{Z})$, $w_1=0$或1，则由$F_S=F_{S_1}$可知$w=w_1$且存在$T\in O_+(F)$使$M_1=TM$。这样可得$S_1=TST^{-1}$。用$S^2=I=(TS)^2=TSTS$，可得$S_1=T^2S$。

(6) 由于F的每一个广义自同构S有形状：$S=TS_0$，这里$T\in O_+(F)$，而S_0为F的一个固定的广义自同构。这样由(1)—(6)所证明的事实可知在同一个Ambiguous类中所含的Ambiguous型的个数是

$$|O_+(F)/O_+^2(F)|=\begin{cases}2, & 如\ d<0;\\ 4, & 如\ d>0.\end{cases}$$

这一等式可见之于引理1.6。引理证毕。

由定义，容易算出下面的引理。

引理1.9 设λ为判别式d的不同奇素因子的个数，则判别式为d的Ambiguous原型的个数如下表所示：

$w=0$的称为是第一类的，$w=1$的称为是第二类的。

d	第一类个数	第二类个数	总数
d奇	0	$2^{\lambda+1}$	$2^{\lambda+1}$
$4\mid d$ 且 $\frac{d}{4}\equiv 1 \pmod 4$	$2^{\lambda+1}$	0	$2^{\lambda+1}$
$4\mid d$ 且 $\frac{d}{4}\equiv 3 \pmod 4$	$2^{\lambda+1}$	$2^{\lambda+1}$	$2^{\lambda+2}$
$8\mid d$，但$32\nmid d$	$2^{\lambda+2}$	0	$2^{\lambda+2}$
$32\mid d$	$2^{\lambda+2}$	$2^{\lambda+2}$	$2^{\lambda+3}$

对判别式为d的二元二次原型类群$\mathscr{C}(d)$，作下列映射

$$\varphi:\ \mathscr{C}(d)\longrightarrow\mathscr{C}(d),$$
$$\varphi(\mathfrak{A})=\mathfrak{A}^2,\ \forall\mathfrak{A}\in\mathscr{C}(d).$$

φ显然是一个群同态。φ的象记为$\mathscr{C}(d)^2$，φ的核是

$$\mathscr{A}(d)=\{\mathfrak{A}\in\mathscr{C}(d)\mid\mathfrak{A}^2=[1]\},$$

即$\mathscr{A}(d)$正是由全体Ambiguous类组成的一个群，它是$\mathscr{C}(d)$的一个子群，它同构于商群$\mathscr{C}(d)/\mathscr{C}(d)^2$，即有

$$\mathscr{A}(d)\cong\mathscr{C}(d)/\mathscr{C}(d)^2.$$

$\mathscr{C}(d)/\mathscr{C}(d)^2$称为判别式为$d$的二元二次原型的族群(genera, genus group)，它的每一个元素是$\mathscr{C}(d)\bmod\mathscr{C}(d)^2$的一个陪集，

称为一个二元二次原型族，简称为族。特别可见每一个族中所含的类的个数都相同。主类[1]所在的族，称为主族，主族中的每一个类都是某一个类的平方。

定理 1.5 记

$$g(d)=|\mathscr{A}(d)|=|\mathscr{C}(d)|\mathscr{C}(d)^2|.$$

则有

$$4g(d)=\lambda(d),$$

其中 $\lambda(d)$ 为引理 1.9 的表的最后一列。

证明 这是上述引理 1.8 与引理1.9的推论，并应注意当$d<0$时，上述提及的表的最后一列的一半才是正定型的总数（其余一半是负定型）。

引理 1.10 设对判别式为 d 的二元二次原型 $f=((a,b,c))$，二次同余方程

$$ax^2+bxy+cy^2\equiv 1(\bmod |d|)$$

有解，那么存在整数 $x,\ y,\ z$ 使

$$ax^2+bxy+cy^2=z^2,$$

并且 $z\neq 0$, $g.c.d.(z,\ d)=1$.

证明 由假设即知存在整数 $x_0,\ y_0,\ n$ 使

$$ax_0^2+bx_0y_0+cy_0^2=1-nd.$$

于是整系数三元二次型

$$F(x,\ y,\ z)=ax^2+bxy+cy^2+x_0yz-y_0zx+nz^2$$

的判别式（参考 G.L. Watson[108]）是 $d(F)=1$。于是由 G.L. Watson p.19 的 Th.10，即知 Min $F=0$，再由该书 p.21 的 Th.13，即知存在 $U\in SL_3(\boldsymbol{Z})$ 使

$$F[U](x,\ y,\ z)=y(Ax+By+Cz)+Dz^2,$$

$$|B|,\ |C|\leqslant\frac{1}{2}A,\qquad A,\ B,\ C,\ D\in Z.$$

由 $d(F[U])=d(F)=1$，即知 $A^2D=1$，故 $A=D=1$，$B=C=0$，即有

$$F[U](x,\ y,\ z)=xy+z^2.$$

再取

$$V=\begin{pmatrix}-1&0&0\\0&0&1\\0&1&0\end{pmatrix}\in SL_3(\mathbb{Z}),$$

即有

$$G(x,\ y,\ z)=F[UV](x,\ y,\ z)=y^2-xz. \tag{2.53}$$

于是命

$$M=(UV)^{-1}=\begin{pmatrix}r_1&s_1&t_1\\r_2&s_2&t_2\\r_3&s_3&t_3\end{pmatrix}\in SL_3(\mathbb{Z}),$$

即有

$$\begin{aligned}f(X,\ Y)=F(X,\ Y,\ 0)&=G[M](X,\ Y,\ 0)\\&=(r_2X+s_2Y)^2-(r_1X+s_1Y)(r_3X+s_3Y).\end{aligned} \tag{2.54}$$

由

$$1=\det M=(r_1s_2-r_2s_1)t_1-(r_1s_3-r_3s_1)t_2+(r_2s_3-r_3s_2)t_3$$

知

$$g.c.d.(r_1s_2-r_2s_1,\ r_1s_3-r_3s_1,\ r_2s_3-r_3s_2)=1.$$

于是由定理1.4的证明中列举的引理可知，存在

$$\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}\in SL_2(\mathbb{Z})$$

使

$$\begin{aligned}g.c.d.(&(r_1s_2-r_2s_1)\alpha^2+(r_1s_3-r_3s_1)\alpha\gamma\\&+(r_2s_3-r_3s_2)\gamma^2,\ 2d)=1.\end{aligned} \tag{2.55}$$

命

$$\sigma=\begin{pmatrix}\alpha^2&2\alpha\gamma&\gamma^2\\\alpha\beta&\alpha\delta+\beta\gamma&\gamma\delta\\\beta^2&2\beta\delta&\delta^2\end{pmatrix},$$

则容易验证

$$\sigma\in Sl_3(\mathbb{Z}),\ G[\sigma](X,\ Y,\ Z)=G(X,\ Y,\ Z). \tag{2.56}$$

命

$$\sigma M=\begin{pmatrix} r_1' & s_1' & t_1' \\ r_2' & s_2' & t_2' \\ r_3' & s_3' & t_3' \end{pmatrix}, \tag{2.57}$$

则有

$$r_1's_2'-r_2's_1'=(r_1s_2-r_2s_1)\alpha^2+(r_1s_3-r_3s_1)\alpha\gamma$$
$$+(r_2s_3-r_3s_2)\gamma^2,$$

故由(2.55)有

$$g.c.d.(r_1's_2'-r_2's_1',\ 2d)=1. \tag{2.58}$$

再由(2.53)、(2.54)、(2.56)与(2.57)即有

$$\begin{aligned} f(X,\ Y)&=F(X,\ Y,\ 0)=G[M](X,\ Y,\ 0)\\ &=(G[\sigma][M])(X,\ Y,\ 0)\\ &=G[\sigma M](X,\ Y,\ 0)\\ &=(r_2'X+s_2'Y)^2-(r_1'X+s_1'Y)(r_3'X+s_3'Y). \end{aligned} \tag{2.59}$$

由(2.58)及(2.59)即知

$$f(s_1',\ -r_1')=(r_2's_1'-r_1's_2')^2=z^2,\ \text{且}\ g.c.d.(z,\ 2d)=1,$$

得到所需。引理获证。

定义 1.5 设 $q>1$ 为一给定的正整数，两个二元二次型 $f=f(x,y)=((a,b,c))=ax^2+bxy+cy^2$ 和 $F=F(x,y)=((A,B,C))=Ax^2+Bxy+Cy^2$ 称为 mod q 相似的，并记为 $f\approx F(\bmod\ q)$，如果存在整系数线性变换

$$x=rX+sY,\ y=tX+uY,$$
$$g.c.d.(ru-st,\ q)=1,$$

使

$$ax^2+bxy+cy^2\equiv AX^2+BXY+CY^2(\bmod\ q).$$

定理 1.6 两个(同为不定型或同为正定型的)具有相同判别式 d 的二元二次原型 f 与 F 属于同一个族的充要条件是

$$f\approx F(\bmod\ |d|).$$

证明 由族群和 mod q 相似的定义可知，只需证明下列的断

言：

判别式为 d 的二元二次原型 $f=((a,\ b,\ c))$ 属于主族的充要条件是二次同余方程

$$ax^2+bxy+cy^2\equiv 1(\bmod\ |d|)$$

有解(注意主类中有一个主型，它是一个首系数为 1 的 Ambiguous 型)。

充分性：由所给的条件及上述引理 1.10 即知，存在一个正整数 A，使不定方程

$$ax^2+bxy+cy^2=A^2$$

有既约解 $(x,\ y)$。所以有

$$((a,\ b,\ c))\approx((A^2,\ B,\ C)),$$

其中 $B,\ C\in\mathbb{Z}$ 使 $d=B^2-4A^2C$。考虑判别式也为 d 的二元二次型

$$((A,\ B,\ AC))。$$

由合成定理(即定理 1.4)的推论即知有

$$[((A,\ B,\ AC))]^2=[((A^2,\ B,\ C))],$$

所以 f 属于主族。

必要性：如 f 属于主族，则存在一个类 $\mathscr{C}$，使 $f\in\mathscr{C}^2$。由定理 1.4 证明中所举的引理，以及定理 1.4 的推论即知，存在一个正整数 A，它与 d 互素，以及一对既约整数 $(x,\ y)$，使

$$ax^2+bxy+cy^2=A^2,$$

由此证明了开头所说的同余方程有解。

定理证毕。

1.5 二元二次型的 genus 特征

本小节中要用到的 Dirichlet 特征的知识，可参考华罗庚著的《数论导引》的第七章和第十二章，或者本书的下一小节。为在下一小节中证明一个完全特征和公式，本小节的 genus 特征的知识，是必需的。在这两小节中，通常的 Dirichlet 特征的知识也都列举了。

定义 1.6 设 d 为一个判别式，即 $d\equiv 0$ 或 $1\pmod 4$，且 d 不是完全平方。对一个正整数 $m>0$，定义 Kronecker 符号 $\left(\frac{d}{m}\right)$ 如下：

$$\left(\frac{d}{p}\right)=0,\quad \text{如素数 } p\mid d;$$

$$\left(\frac{d}{2}\right)=\begin{cases}1, & \text{如 } d\equiv 1\pmod 8;\\ -1, & \text{如 } d\equiv 5\pmod 8;\end{cases}$$

$$\left(\frac{d}{p}\right)=\text{Legendre 符号，如奇素数 } p\nmid d,$$

即对奇素数 $p\nmid d$，$\left(\frac{d}{p}\right)=1$，如 d 为 mod p 平方剩余，否则 $\left(\frac{d}{p}\right)=-1$；

如 $m=\prod_{j=1}^{s}p_j$，p_j 是素数，则

$$\left(\frac{d}{m}\right)=\prod_{j=1}^{s}\left(\frac{d}{p_j}\right).$$

引理 1.11 我们有

(1) $\left(\frac{d}{m}\right)=0$，如 $g.c.d.(m,\ d)>1$；

$\left(\frac{d}{m}\right)=\pm 1$，如 $g.c.d.(m,\ d)=1$。

(2) 如 $m_1,\ m_2>0$，则 $\left(\frac{d}{m_1m_2}\right)=\left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right)$。

(3) 如 $m>0$，$g.c.d.(m,\ d)=1$，则 Kronecker 符号

$$\left(\frac{d}{m}\right)=\begin{cases}\left(\frac{m}{|d|}\right), & \text{当 } d \text{ 为奇数；}\\ \left(\frac{2}{m}\right)^{b}(-1)^{\frac{u-1}{2}\cdot\frac{m-1}{2}}\left(\frac{m}{|u|}\right), & \text{当 } d=2^{b}u,\ 2\nmid u,\end{cases}$$

其中右边的 $\left(\frac{m}{|d|}\right)$，$\left(\frac{2}{m}\right)$，$\left(\frac{m}{|u|}\right)$ 均为 Jacobi 符号。

(4) $\left(\frac{d}{m}\right)=\left(\frac{d}{|d|+m}\right)$。

(5) Kronecker 符号$\left(\frac{d}{m}\right)$是 mod $|d|$ 的实特征，故它可以以 $|d|$ 为周期地拓展至所有的整数 m，而有

$$\left(\frac{d}{m_1m_2}\right)=\left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right),\quad \forall m_1,\ m_2\in\mathbb{Z}.$$

(6) 设 m、$n>0$，$m\equiv -n(\text{mod }|d|)$，则

$$\left(\frac{d}{m}\right)=\begin{cases}\left(\frac{d}{n}\right), & \text{如 } d>0;\\ -\left(\frac{d}{n}\right), & \text{如 } d<0.\end{cases}$$

证明 以上都不难，连定义均见华罗庚著《数论导引》第十二章。

记 Kronecker 符号 $\chi_d(*)=\left(\frac{d}{*}\right)$。命 $\mathbb{Z}^*_{|d|}=(\mathbb{Z}/|d|\mathbb{Z})^*$，及

$$K_d=\left\{x\in\mathbb{Z}^*_{|d|}\ \middle|\ \begin{array}{l}1.\ x\text{ 为 mod }p\text{ 二次剩余，如奇素数 }p|d,\\ 2.\ x\equiv\begin{cases}1\ (\text{mod }4), & \text{如 } d\equiv 12\ (\text{mod }16),\ \text{或 } 16(\text{mod }32);\\ 1\ (\text{mod }8), & \text{如 } d\equiv 0(\text{mod }32);\\ 1\text{ 或 }7(\text{mod }8), & \text{如 } d\equiv 8(\text{mod }32);\\ 1\text{ 或 }3(\text{mod }8), & \text{如 } d\equiv 24(\text{mod }32).\end{cases}\end{array}\right\}$$

作映射

$$\chi_d:\ \mathbb{Z}^*_{|d|}\longrightarrow\{\pm 1\},$$

则由上述引理 1.11 的(5)，即知 χ_d 为群的同态映射，并且 χ_d 是满映射，所以有

$$\mathbb{Z}^*_{|d|}/\text{Ker }\chi_d\cong\{\pm 1\}.$$

容易验证下列的引理。

引理 1.12 K_d 是 Ker χ_d 的一个子群。

由引理 1.12 可知，χ_d 在 $\mathbb{Z}^*_{|d|}/K_d$ 上诱导出一个群同态 χ'_d：

$$\chi'_d:\mathbb{Z}^*_{|d|}/K_d\longrightarrow\{\pm 1\},$$

并且 χ'_d 也是满映射，从而有

$$\text{Ker }\chi'_d\cong\text{Ker }\chi_d/K_d.$$

引理 1.13 如 $\bar{m}=m(\text{mod }|d|)$，$\bar{n}=n(\text{mod }|d|)$，$\bar{m}$，$\bar{n}\in$

$\mathbb{Z}^*_{|d|}$ 均可由 $\mathscr{C}(d)$ 中的同一个类 $\mathfrak{A}$ 中的型所表出，则有

$$\bar{m}\equiv\bar{n} \bmod K_d。$$

证明　由于显然有 $\bar{n}^2\in K_d$，故只需证明 $\bar{m}\bar{n}\in K_d$。由假设，可取 $f\in\mathfrak{A}$，r，s，t，$u\in\mathbb{Z}$，使

$$f(r,\ s)=m,\ f(t,\ u)=n。$$

考虑 f 在 $\begin{pmatrix} r & t \\ s & u\end{pmatrix}$ 下的判别式，即知存在 l，$x\in\mathbb{Z}$，使

$$l^2-4mn=dx^2。$$

这样分别情况验证，即可证明 $\bar{m}\bar{n}\in K_d$。引理证毕。

由这一引理，对每一个 $\mathfrak{A}\in\mathscr{C}(d)$，以 $\psi(\mathfrak{A})$ 记 $\mathfrak{A}$ 中型所能表出的 $\mathbb{Z}^*_{|d|}$ 中元素 mod K_d 的陪集，这是唯一确定的，从而可以定义映射

$$\psi:\ \mathscr{C}(d)\longrightarrow\mathbb{Z}^*_{|d|}/K_d,$$

ψ 显然是群同态。

定理 1.7　我们有下列的正合序列

$$\longrightarrow\mathscr{A}(d)\xrightarrow{1}\mathscr{C}(d)\xrightarrow{\varphi}\mathscr{C}(d)\xrightarrow{\psi}\mathbb{Z}^*_{|d|}/K_d\xrightarrow{\chi'_d}\{\pm1\}\longrightarrow1。$$

证明　许多事实以前已证明了，剩下来要证明的是：

$$\mathscr{C}(d)^2=\operatorname{Ker}\psi,\ \operatorname{Im}\psi=\operatorname{Ker}\chi'_d。$$

不难证明 $f\in\operatorname{Ker}\psi$ 的充要条件是 f 可以 mod $|d|$ 表出 1，这样由定理 1.6 及其证明开头的说明，即知 $f\in\operatorname{Ker}\psi$ 等价于 f 属于主族。因此得到 $\mathscr{C}(d)^2=\operatorname{Ker}\psi$。

又容易证明

$$\operatorname{Im}\psi\subseteq\operatorname{Ker}\chi'_d，故 |\operatorname{Im}\psi|\leqslant|\operatorname{Ker}\chi'_d|。$$

由

$$(\mathbb{Z}^*_{|d|}/K_d)/\operatorname{Ker}\chi'_d\cong\{\pm1\},$$

即知

$$|\operatorname{Ker}\chi'_d|=\frac{1}{2}|\mathbb{Z}^*_{|d|}/K_d|,$$

又由已证明的，有

$$\mathscr{A}(d)\cong\operatorname{Im}\psi，故|\mathscr{A}(d)|\leqslant\frac{1}{2}|\mathbb{Z}^*_{|d|}/K_d|,$$

因此定理的证明归结为证明下述的引理1.14。

引理1.14 $|\mathscr{A}(d)|=\frac{1}{2}|Z^*_{|d|}/K_d|$.

证明 定理1.5已算出了$|\mathscr{A}(d)|$的值，因此只要证明等式右边与该值相等即可，这是不难完成的。引理证毕。

这样，由定理1.7，可以得到一系列的同构：

$$\mathscr{A}(d)\cong\mathscr{C}(d)/\mathscr{C}(d)^2\cong\text{Ker}\chi'_d\cong\text{Ker }\chi_d/K_d.$$

由于$\mathscr{A}(d)$中的元素都是1阶或2阶的，这样得到下面的断言。

断言 如$\bar{m}=m(\text{mod }|d|)\in\text{Ker }\chi_d$，则$\bar{m}^2\in K_d$.

现在考虑族群$\mathscr{C}(d)/\mathscr{C}(d)^2$的特征$\chi$，这个特征称为类群$\mathscr{C}(d)$的genus特征（实际上$\chi$在$\mathscr{C}(d)$上诱导了一个特征，后者在平方类上取值为1，我们可把两者混同对待）。由上述同构可知，不妨设χ即为$\text{Ker }\chi_d/K_d$的特征，由于$\text{Ker }\chi_d\subseteq Z^*_{|d|}$，所以可以认为$\chi$是一个mod $|d|$的Dirichlet特征，它在K_d的每一个元素处取值为1。再由上述断言即知χ应是一个实特征，根据Dirichlet的一条定理（见文献[11]p.37）即知，它应为某一个Kronecker符号$\left(\frac{d_1}{*}\right)$，这里$d_1|d$，再结合$K_d$的构造，可知，存在一个正整数$k$，$k|d$，使$\chi$为一个mod k的一个实的Dirichlet特征，并且其特征分解式（参考华罗庚著《数论导引》第七章或本书下一小节）如下：

令$k=\prod\limits_{p|k}k_p$，$k_p=p^{\alpha_p}$，为k的标准分解式，$\chi=\prod\limits_{p|k}\chi_p$为相应的特征分解式，$\chi_p$为mod k_p的Dirichlet实特征，并且：

当p为奇素数时，χ_p的导子为p，同时$\chi_p(*)=\left(\frac{*}{p}\right)$是mod p的Legendre符号；

当$p=2$时，χ_2的导子是$2^\alpha=4$或8，同时$\chi_2(*)=$Kronecker符号$\left(\frac{-4}{*}\right)$、$\left(\frac{8}{*}\right)$或$\left(\frac{-8}{*}\right)$，并且$\frac{d}{2^\alpha}\equiv0$或$\chi_2(-1)\ (\text{mod }4)$。

附注 当χ为mod $|d|$主特征时，取$k=1$。

注意这样的mod k特征中有一些是彼此在$\text{Ker }\chi_d$上取值完

全相同的，如其取值完全相同，则是 $\mathrm{Ker}\,\chi_d/K_d$ 的同一个特征。

另外，确切地说，$\mathscr{C}(d)/\mathscr{C}(d)^2$ 的一个特征，即 $\mathscr{C}(d)$ 的一个 genus 特征，是上述所描述的特征 χ 在 $\psi(\mathfrak{A})$ ($\mathfrak{A}\in\mathscr{C}(d)/\mathscr{C}(d)^2$) 处所取的值确定的，即对 $\mathfrak{A}\in\mathscr{C}(d)/\mathscr{C}(d)^2$，令 m 为 $\mathfrak{A}$ 所取的与 d 互素的整数，则 $\chi(\mathfrak{A})=\chi(m)$。

由 Abel 群的基本理论可知：这种特征彼此不同的个数即为 $\mathscr{C}(d)/\mathscr{C}(d)^2$ 的阶，即 $|\mathscr{A}(d)|=g(d)$。

上述对于 genus 特征的刻划，如用 Hilbert 符号，则形式上会更简单一些，即我们有

引理 1.15 设 $f=((a,\ b,\ c))$ 是一个判别式为 d 的二元二次原型，则对 $\mathscr{C}(d)/\mathscr{C}(d)^2$ 的一个特征（即 $\mathscr{C}(d)$ 的一个 genus 特征）χ，有

$$\chi([f])=\prod_{p\mid P(\chi)}(d,\ a)_p,$$

这里 $P(\chi)$ 为由 χ 决定的由 d 的某些素因子组成的素数集合，而对每一个素数 p，$(*,\ *)_p$ 是 mod p 的 Hilbert 符号，其定义如下：

定义 1.7 对一个素数 p 和两个非零的整数 a，b，mod p 的 Hilbert 符号 $(a,\ b)_p$ 定义为

$$(a,\ b)_p=\begin{cases}1, & \text{如 } ax^2+by^2 \text{ 能表出一个 } p\text{-adic 平方数；}\\ -1, & \text{否则。}\end{cases}$$

这里 ax^2+by^2 能表出一个 p-adic 平方数的意义是指：对于素数 p 的任一个幂 $p^n(n\geqslant1)$，三元二次同余方程

$$ax^2+by^2\equiv z^2(\mathrm{mod}\ \ p^n)$$

均有整数解。

引理 1.16 (Hilbert 符号的性质)我们有

(1) $(a,\ b)_p=(b,\ a)_p$；

(2) $(a,\ b)_p=(a,\ -ab)_p$；

(3) $(a,\ b)_p=(a',\ b)_p$，如 aa' 是一个 p-adic 平方数；

(4) $(a,\ b)_p(a',\ b)_p=(aa',\ b)_p$；

(5) 当 $p\nmid ab$ 时，有

$$(a,\ b)_p=\begin{cases}\left(\dfrac{a}{p}\right)(\text{mod } p \text{ 的 Legendre 符号}), \text{如} p\nmid 2a,\ p\| b;\\ 1,\ \text{如 } p=2\| b,\ \text{且 } a \text{ 或 } a+b\equiv 1 \pmod 8;\\ -1,\ \text{其他};\end{cases}$$

(6) $(a,\ b)_2=\begin{cases}1,\ \text{如 } a\equiv 1 \pmod 4,\ \text{且 } b \text{ 奇};\\ -1,\ \text{如 } a\equiv b\equiv -1 \pmod 4,\end{cases}$

(7) $(a,\ b)_p=1$, 如 $p\nmid 2ab$;

(8) 对 $p=\infty$, 约定

$$(a,\ b)_\infty=\begin{cases}1,\ \text{如 } ab\neq 0,\ \text{且 } a \text{ 或 } b>0;\\ -1,\ \text{如 } a<0 \text{ 且 } b<0;\end{cases}$$

(9) $\prod\limits_p (a,\ b)_p=1$, 这里 p 跑过 ∞ 及所有素数。

证明 定义与证明可见 G.L.Watson 的书[108]。

我们还可证明下面的引理。

引理 1.17 设 $f=((a,\ b,\ c))$ 是一个判别式为 d 的二元二次原型，则对 d 的每一个素因子 p, 有:

$$(d,a)_p=\begin{cases}\left(\dfrac{a}{p}\right) \text{或} \left(\dfrac{c}{p}\right) (\text{mod } p \text{ 的 Legendre 符号}), \text{如 } p \text{ 奇},\\ \quad \text{且 } p\nmid a \text{ 或 } p\nmid c;\\ \left(\dfrac{k}{a}\right) \text{或} \left(\dfrac{k}{c}\right) (\text{Kronecker 符号}), \text{如 } p=2,\ k=-4\\ \quad \text{或 } \pm 8,\ k\mid d,\ \dfrac{d}{k}\equiv 1 \pmod 4, \text{且 } a \text{ 或 } c \text{ 奇}.\end{cases}$$

1.6 一个完全特征和公式

为叙述和引用的方便，我们列举 Dirichlet 特征的一些知识，这可参考华罗庚著《数论导引》或潘承洞和潘承彪著《解析数论基础》。

对一个正整数 k, 共有 $\varphi(k)$ (Euler 函数) 个 mod k 的 Dirichlet 特征，今后简称为 mod k 特征，它们是如下定义的:

定义 1.8 对一个给定的正整数 k, 一个 mod k 的特征 χ, 定义为由 $\mathbb{Z}_k^*=(\mathbb{Z}/k\mathbb{Z})^*$ 到 $\mathscr{C}^*$ 的一个同态。确切地说，χ 是 $n\in\mathbb{Z}$

的一个函数，它满足

(1) $|\chi(n)|=1$, 对 $n\in\mathbb{Z}$ 且 $g.c.d.(n, k)=1$;

(2) $\chi(1)=1$; $\chi(n)=0$, 如 $g.c.d.(n, k)>1$;

(3) $\chi(a)=\chi(b)$, 如 $a\equiv b \pmod{k}$;

(4) $\chi(ab)=\chi(a)\chi(b)$, 如 $a, b\in\mathbb{Z}$;

(5) 如 $\chi(n)=1$, 对每一个与 k 互素的整数 n 都成立，则称 χ 为 mod k 的主特征，记为 χ_0。

这 $\varphi(k)$ 个特征可如下地构造：

(1) 如 $k=p^l$, p 为奇素数，l 为正整数。此时令 g 为 mod p^l 的一个原根。当 $p\nmid n$ 时，可以定义 ind n, 即有

$$n\equiv g^{\text{ind}\, n} \pmod{p^l}.$$

这样可得 $\varphi(p^l)$ 个 mod p^l 特征：

$$\chi_a(n)=e^{2\pi i a\,\text{ind} n/\varphi(p^l)},\ 1\leqslant a\leqslant\varphi(p^l).$$

(2) 如 $k=2^l$, l 为正整数，则有下列三种情形：

(2.1) 如 $l=1$, 则只有一个主特征。

(2.2) $l=2$ 时，除主特征 χ_0 处，还有一个特征 χ:

$\chi(1)=1$, $\chi(3)=-1$, 即 $\chi(n)=\left(\frac{-4}{n}\right)$为 Kronecker 符号。

(2.3) $l\geqslant 3$, 当 n 为一个奇数时，存在整数 b 使

$$n\equiv(-1)^{\frac{1}{2}(n-1)}5^b \pmod{2^l},\ b\geqslant 0.$$

定义

$$\chi_{a,c}(n)=(-1)^{\frac{1}{2}(n-1)a}e^{2\pi i c b/2^{l-2}},$$

这里 a mod 2 有二个不同值，c mod 2^{l-2} 有 2^{l-2} 个不同值，这样可得 $\varphi(2^l)=2^{l-1}$ 个 mod 2^l 特征。

(3) 一般情形，令

$$k=p_1^{l_1}\cdots p_s^{l_s},\ l_\nu>0,$$

是 k 的标准分解式。

取 mod $p_\nu^{l_\nu}$ 的一个特征，为 $\chi^{(\nu)}(n)$, 则

$$\chi(n)=\prod_{\nu=1}^{s}\chi^{(\nu)}(n)$$

为 mod k 的一个特征，由此可得 $\varphi(k)$个 mod k 的特征。

反之，如特征 $\chi(n)$的模为 $k=k_1\cdots k_s$，这里 $k_1, \cdots, k_s$ 两两互素，则存在以 $k_\nu(\nu=1, \cdots, s)$为模的特征 $\chi_\nu(n)$，使

$$\chi(n)=\prod_{\nu=1}^{s}\chi_\nu(n).$$

引理 1.18 我们有

$$\sum_{n(\bmod k)}\chi(n)=\begin{cases}\varphi(k), & \text{如 } \chi=\chi_0;\\ 0, & \text{如 } \chi\neq\chi_0.\end{cases}$$

$$\sum_{\chi}\chi(n)=\begin{cases}\varphi(k), & \text{如 } n\equiv 1 \pmod k;\\ 0, & \text{如 } n\not\equiv 1 \pmod k,\end{cases}$$

其中前一个求和中 n 跑过 mod k 的一个完全剩余组，后一求和中 χ 跑过 mod k 的有 $\varphi(k)$个彼此不同的特征。

定义 1.9 设 χ 为 mod k 的特征。χ 称为 mod k 的非原特征，如果存在 k 的一个正的真因子 M，使

$\chi(n)=\chi(n')$， 如 $n\equiv n' \pmod M$ 且 $g.c.d.(n, k) = g.c.d.(n', k)=1$；否则就称 χ 为 mod k 的原特征。

定义 1.10 对 mod k 的特征 χ，如下定义的正整数 M，

$M=\min\{m|1\leqslant m|k,\ \chi(n)=1$ 如 $n\equiv 1 \pmod m$ 且 $g.c.d.(n, k)=1\}$称为 χ 的导子(conductor)。

引理 1.19 设 χ 为 mod k 特征，则 χ 的导子等于

$$\min\{m|1\leqslant m|k,\ \chi(n)=\chi(n') \text{ 如 } n\equiv n' \pmod m$$

且 $$g.c.d.(n, k)=g.c.d.(n', k)=1\}.$$

引理 1.20 (1) 一个 mod k 的特征 χ 是 mod k 的原特征的充要条件是 χ 的导子等于 k。

(2) 设 mod k 的特征 χ 的导子为 M，则存在一个 mod M 的原特征 χ_1，使 $\chi(n)=\chi_1(n)$，如 $g.c.d.(n, k)=1$。这个 χ_1 称为等价于 χ 的原特征。

引理 1.21 Kronecker 符号 $\left(\frac{d}{n}\right)$为 mod$|d|$的实特征；反之每个实特征必为某个判别式的 Kronecker符号。当 d 为基本判别式时，即有 $d=d_0$，若 $d_0\equiv 1 \pmod 4$；或 $d=4d_0$，如 $d_0\equiv 2$ 或 3

(mod 4)，而 d_0 是无平方因子时，Kronecker 符号 $\left(\frac{d}{n}\right)$ 为一个 mod $|d|$ 的实原特征；反之，每个实原特征，一定是某个基本判别式 d 的 Kronecker 符号 $\left(\frac{d}{n}\right)$。注意 $d\neq 1$。

定义 1.11 设 d 为一个判别式，即 $d\equiv 0$ 或 $1 \pmod 4$，且 d 不是完全平方；$\mathscr{C}(d)$ 是判别式为 d 的二元二次原型类群（$d<0$ 时只考虑正定型）；χ 是 mod k 的非主特征，且设 χ 的特征分解式为

$\chi=\prod_{p|k}\chi_p$，$k=\prod_{p|k}k_p$ 为 k 的标准分解式，χ_p 为 mod k_p 的特征。

χ 称为 $\mathscr{C}(d)$ 的一个 genus 特征，如果对 k 的每一个素因子 p，均有 $p|d$，且满足下列条件：

当 p 为奇素数时，χ_p 的导子为 p，且 $\chi_p(n)=\left(\frac{n}{p}\right)$ 是 mod p 的 Legendre 符号；

当 $p=2$ 时，χ_2 的导子 $=2^\alpha=4$ 或 8，且 $\chi_2(n)=\left(\frac{-4}{n}\right)$，$\left(\frac{8}{n}\right)$ 或 $\left(\frac{-8}{n}\right)$（均是 Kronecker 符号），同时还有 $2^\alpha|d$，且

$$\frac{d}{2^\alpha}\equiv 0 \text{ 或 } \chi_2(-1) \pmod 4。$$

附注 不难看出，当 d 为一个基本判别式时，一个 mod k 的特征 χ 是 $\mathscr{C}(d)$ 的一个 genus 特征当且仅当 $k|d$，k 是一个基本判别式，且 $\frac{d}{k}=1$ 或也是一个基本判别式，同时 χ 为 Kronecker 符号 $\chi(*)=\left(\frac{k}{*}\right)$。

以上所有的定义与引理的证明可参考上述指出的文献，最后一个定义实际是上一小节的内容之一。

本小节的任务是证明下述的定理。

定理 1.8 设 χ 为一个 mod k 的 Dirichlet 特征，$f(x, y)=ax^2+bxy+cy^2$ 是一个判别式为 $d=b^2-4ac$ 的（整系数）二元二次

原型,即 $g.c.d.(a, b, c)=1$($d<0$ 时,只考虑正定型)。那么我们有

$$\frac{1}{k\varphi(k)}\sum_{m,n(\bmod k)}\chi(f(m,n))$$

$$=\begin{cases}\chi_1([f])\prod_{p|k_0}\left(1-\left(\frac{d}{p}\right)\right), & \text{如}\chi\text{可分解为}\chi=\chi_0\chi_1,\text{其中}\chi_0\text{为}\bmod k_0\text{的主特征},\chi_1\text{是}\mathscr{C}(d)\text{的一个 genus 特征;}\\ 0 & ,\text{否则,}\end{cases}$$

这里 φ 为Euler函数,$\left(\frac{d}{*}\right)$为 Kronecker 符号,$\mathscr{C}(d)$ 是判别式为 d 的二元二次原型类群($d<0$ 时,只考虑正定型),$[f]$是 f 所属的类,$\chi_1([f])=\chi_1(A)$,如整数 A 能被 f 所表出且 $g.c.d.(A, d)=1$。

附注 我们也记 $\chi_1(f)=\chi_1([f])$。

在证明定理之前,先证明一些引理。

引理 1.22 设 p 为奇素数,整数 $\alpha\geqslant1$,χ 为 $\bmod\ p^{\alpha+1}$ 的非主特征,则有

$$\sum_{m(\bmod p)}\chi(p^\alpha m+n)=\begin{cases}0, & \text{如}\chi\text{为}\bmod\ p^{\alpha+1}\text{原特征;}\\ p\chi_1(n), & \text{否则,}\end{cases}$$

这里 χ 为 $\bmod\ p^{\alpha+1}$ 的非原特征时,χ_1 为一个 $\bmod\ p^\alpha$ 的非主特征,其定义见之于以下的证明中。

证明 (1) 设 χ 为 $\bmod p^{\alpha+1}$ 的原特征,则$\bar{\chi}(\bar{\chi}(n)\overset{\text{def}}{=}\overline{\chi(n)})$ 也是 $\bmod\ p^{\alpha+1}$ 的原特征,且 Gauss 和 $\tau(\chi)=\sum_{u(p^{\alpha+1})}\chi(u)e^{2\pi iu/p^{\alpha+1}}$,满足 $|\tau(\chi)|=p^{\frac{\alpha+1}{2}}$,同样$|\tau(\bar{\chi})|=p^{\frac{\alpha+1}{2}}$。从而有

$$\chi(\nu)=\frac{1}{\tau(\bar{\chi})}\sum_{u(\bmod p^{\alpha+1})}\bar{\chi}(u)e^{2\pi iu\nu/p^{\alpha+1}},$$

所以得到

$$\sum_{m(\bmod p)}\chi(p^\alpha m+n)=\frac{1}{\tau(\bar{\chi})}\sum_{u(\bmod p^{\alpha+1})}\bar{\chi}(u)e^{2\pi iun/p^{\alpha+1}}\sum_{m(\bmod p)}e^{2\pi ium/p}$$

$$=0,$$

这是因为当 $p\nmid u$ 时，内和为零，而当 $p|u$ 时，$\bar{\chi}(u)=0$。

(2) 设 χ 为 mod $p^{\alpha+1}$ 的非原特征。令 g 为 mod $p^{\alpha+1}$ 的一个原根。对 $p\nmid n$，有 $\chi(n)=e^{2\pi i a\,\mathrm{ind}\,n/\varphi(p^{\alpha+1})}$，这里 a 是一个整数，它满足 $1\leqslant a<\varphi(p^{\alpha+1})$。由于 χ 为 mod $p^{\alpha+1}$ 的非原特征，故 $p|a$。令 $a=a_1p$，a_1 是一个整数，它满足 $1\leqslant a_1<\varphi(p^{\alpha})$。对 $p\nmid n$，令 m $=\mathrm{ind}(p^{\alpha}m+n)$，$1\leqslant m'\leqslant\varphi(p^{\alpha+1})$。

又 g 也是 mod p^{α} 的一个原根，令 n mod $p^{\alpha}(p\nmid n)$ 而言的 $\mathrm{inde}\,\chi=\widetilde{\mathrm{ind}}\,n=m''$，$1\leqslant m''\leqslant\varphi(p^{\alpha})$，即得

$$p^{\alpha}m+n\equiv g^{m'}\ (\mathrm{mod}\ p^{\alpha+1}),$$

$$n\equiv g^{m''}\ (\mathrm{mod}\ p^{\alpha}),$$

所以有

$$m'\equiv m''\ (\mathrm{mod}\ \varphi(p^{\alpha})),$$

因此有

$$\chi(p^{\alpha m+n})=e^{2\pi i a m'/\varphi(p^{\alpha+1})}=e^{2\pi i a_1 m'/\varphi(p^{\alpha})}$$

$$=e^{2\pi i a_1 m''/\varphi(p^{\alpha})}=\chi_1(n),$$

这里 χ_1 为一个 mod p^{α} 的非主特征，从而有

$$\sum_{m(\mathrm{mod}\ p)}\chi(p^{\alpha m+n})=p\chi_1(n).$$

引理证毕。

引理 1.23 设 p 为奇素数，χ 为 mod p 的非主特征，$f(x,y)=ax^2+bxy+cy^2$ 是一个判别式为 d 的二元二次原型，则有

$$\sum_{m,n(\mathrm{mod}\ p)}\chi(f(m,n))$$

$$=\begin{cases}0, & \text{当 } p\nmid d，\text{或 } p|d \text{ 而 } \chi\neq\rho \text{ 时；}\\ p(p-1)\chi(a)\text{ 或 }p(p-1)\chi(c), & \text{当 } p|d，\text{且 } \chi=\rho \text{ 而 } p\nmid a \text{ 或 } p\nmid c \text{ 时，}\end{cases}$$

这里 ρ 为 mod p 的 Legendre 符号。

证明 (1) 当 a，c 同时被 p 除尽时，左边的和为

$$\chi(b)\Big(\sum_{m(\mathrm{mod}\ p)}\chi(m)\Big)^2=0.$$

(2) 当 a，c 不同时被 p 除尽时，由对称性，不妨设 $p\nmid a$，这时有

$$\chi(4a)\sum_{m,n(\bmod p)}\chi(f(m,n)) = \sum_{m,n(\bmod p)}\chi((2am+bn)^2-dn^2)$$
$$=\sum_{m,n(\bmod p)}\chi(m^2-dn^2).$$

(2)′ 当 $p|d$ 时，

$$\sum_{m,n(\bmod p)}\chi(m^2-dn^2)=pS(\chi^2),$$

这里对 mod p 的特征 ξ，定义

$$S(\xi)=\sum_{m(\bmod p)}\xi(n).$$

易见，这时有

$$\sum_{m,n(\bmod p)}\chi(m^2-dn^2)$$
$$=\begin{cases}0\quad ,\text{如 }\chi^2\text{ 不是 mod } p\text{ 的主特征;}\\ p\varphi(p),\text{如 }\chi^2\text{ 是 mod } p\text{ 的主特征,}\end{cases}$$
$$=\begin{cases}0\quad ,\text{如 }\chi\neq\rho;\\ p(p-1),\text{如 }\chi=\rho.\end{cases}$$

其中 ρ 为 mod p 的 Legendre 符号。

(2)″ 当 $p\nmid d$ 时，

$$\sum_{m,n(\bmod p)}\chi(m^2-dn^2)=\sum_{m(\bmod p)}\chi(m^2)+\sum_{\substack{n(\bmod p)\\ p\nmid n}}\sum_{m(\bmod p)}\chi(m^2-dn^2)$$
$$=S(\chi^2)+\sum_{n(\bmod p)}\chi(n^2)\sum_{m(\bmod p)}\chi(m^2-d)$$
$$=S(\chi^2)\Big(1+\sum_{m(\bmod p)}\chi(m^2-d)\Big),$$

又当 $p\nmid d$ 时，有

$$\sum_{m(\bmod p)}\chi(m^2-d)=\sum_{m(\bmod p)}\chi(m-d)(1+\rho(m))$$
$$=\sum_{m(\bmod p)}\chi(m-d)\rho(m)$$
$$=\chi(d)\rho(d)\sum_{m(\bmod p)}\chi(m-1)\rho(m)$$
$$=\chi(-d)\rho(d)\sum_{m(\bmod p)}\chi(1-m)\rho(m)$$
$$=\chi(-d)\rho(d)J(\chi,\rho),$$

这里 $J(\chi,\rho)$是 Jacobi 和，对非主特征 χ，有

$$J(\chi,\ \rho)=\begin{cases}-\chi(-1)\ , & 如\ \chi=\rho;\\ \dfrac{\tau(\chi)\tau(\rho)}{\tau(\chi\rho)}, & 如\ \chi\neq\rho.\end{cases}$$

这儿 $\tau(\xi)$ 是关于 mod p 特征 ξ 的 Gauss 和，已于上面定义过。以上这些可见 Ireland 与 Rosen 所著的书[39]p.93。

于是 $p\nmid d$ 时，有

$$\sum_{m,n(\bmod p)}\chi(m^2-dn^2)=S(\chi^2)(1+\chi(-d)\rho(d)J(\chi,\ \rho))=0,$$

这是因为当 $\chi=\rho$ 时，$J(\chi,\ \rho)=-\chi(-1)$；而当 $\chi\neq\rho$ 时，$S(\chi^2)=0$。

综上所述，引理证毕。

引理 1.24 设 p 为奇素数，α 为正整数，χ 为 mod p^α 的非主特征，$f(x,\ y)=ax^2+bxy+cy^2$ 是一个判别式为 d 的二元二次原型，则有

$$\sum_{m,n(\bmod p^\alpha)}\chi(f(m,\ n))$$

$$=\begin{cases}p^\alpha\varphi(p^\alpha)\cdot\begin{cases}\chi(a)\\ 或\ \chi(c)\end{cases}, & 如\ p\mid d,\ 且\ \chi\ 的导子为\ p,\ \chi\ 等价于\ \rho,\ 同时\ p\nmid a\ 或\ p\nmid c;\\ 0 & ,其他,\end{cases}$$

其中 ρ 为 mod p 的 Legendre 符号。

证明 当 $\alpha=1$ 时，由引理 1.23 已知本引理成立。以下对 $\alpha+1\geqslant 2$ 用归纳法，即设 $\alpha\geqslant 1$ 时引理已成立，现来证明引理对 $\alpha+1$ 也成立。

(1) $a,\ c$ 不同时为 p 除尽时，不妨设 $p\nmid a$ 时，故有

$$\chi(4a)\sum_{m,n(\bmod p^{\alpha+1})}\chi(f(m,\ n))=\sum_{m,n(\bmod p^{\alpha+1})}\chi((2am+bn)^2-dn^2)$$

$$=\sum_{m,n(\bmod p^{\alpha+1})}\chi(m^2-dn^2).$$

令

$$m=p^\alpha m_1+m_2,\ m_1(\bmod\ p),\ 1\leqslant m_2\leqslant p^\alpha,$$

$$n=p^\alpha n_1+n_2,\ n_1(\bmod\ p),\ 1\leqslant n_2\leqslant p^\alpha.$$

则有

$$\sum_{m,n(\bmod p^{\alpha+1})}\chi(m^2-dn^2)$$
$$=\sum_{1\leqslant m_2,n_2\leqslant p^\alpha}\ \sum_{m_1,n_1(\bmod p)}\chi(p^\alpha(2m_1m_2-2dn_1n_2)+m_2^2-dn_2^2),$$

由引理 1.22 知,当 χ 为 $\bmod\ p^{\alpha+1}$ 的原特征时,内和等于 0, 这是因为当 $p\nmid m_2$ 或 $p\nmid dn_2$ 时, 整个内和等于 0, 而当 $p|m_2$ 且 $p|dn_2$ 时,内和的每一项都是 0。 仍由引理 1.22 知,当 χ 为 $\bmod\ p^{\alpha+1}$ 的非原特征时,内和等于 $p^2\chi_1(m_2^2-dn_2^2)$, 其中 χ_1 为一个 $\bmod\ p^\alpha$ 的非主特征,如引理 1.22 证明中所定义的。

这样有

$$\sum_{m,n(\bmod p^{\alpha+1})}\chi(m^2-dn^2)$$
$$=\begin{cases}p^2\displaystyle\sum_{m,n(\bmod p^\alpha)}\chi_1(m^2-dn^2), & \text{如 }\chi\text{ 为 }\bmod\ p^{\alpha+1}\text{ 的非原特征;}\\ 0, & \text{如 }\chi\text{ 为 }\bmod\ p^{\alpha+1}\text{ 的原特征,}\end{cases}$$

在前一种情况下, χ_1 为一个 $\bmod\ p^\alpha$ 的非主特征, 其定义见引理 1.22 的证明。于是由归纳假设及 χ_1 的定义, 可知在这种情况下, 引理对 $\alpha+1$ 已证。

(2) 当 $p|a,\ c$ 时, 若 $p|b$ 则引理显然成立, 故可设 $p\nmid b$, 从而 $p\nmid d$。令

$$m=m_1p^\alpha+m_2,\ n=n_1p^\alpha+n_2,$$
$$m_1,\ n_1(\bmod p),\ 1\leqslant m_2,\ n_2\leqslant p^\alpha.$$

则有

$$\sum_{m,n(\bmod p^{\alpha+1})}\chi(f(m,\ n))$$
$$=\sum_{1\leqslant m_2,n_2\leqslant p^\alpha}\ \sum_{m_1,n_1(\bmod p)}\chi(f(m_2,\ n_2)+bp^\alpha(m_1n_2+m_2n_1))$$
$$=\sum_{1\leqslant m_2,n_2\leqslant p^\alpha}\ \sum_{m_1,n_1(\bmod p)}\chi(f(m_2,\ n_2)+p^\alpha(m_1n_2+m_2n_1)),$$

由引理 1.22 可知,内和(注意 $p|a,\ c$)

$$=\begin{cases}0, & \text{如 }\chi\text{ 为 }\bmod\ p^{\alpha+1}\text{ 原特征;}\\ p^2\chi_1(f(m_2,\ n_2)), & \text{如 }\chi\text{ 为 }\bmod\ p^{\alpha+1}\text{ 非原特征,}\end{cases}$$

在后一种情形下, χ_1 为一个 $\bmod\ p^\alpha$ 的非主特征, 其定义见引理 1.22 的证明。因此有

$$\sum_{m,n(\text{mod }p^{\alpha+1})}\chi(f(m,n))$$
$$=\begin{cases}0\,, & \text{如 }\chi\text{ 为 mod }p^{\alpha+1}\text{ 原特征;}\\ p^2\sum\limits_{m,n(\text{mod }p^{\alpha})}\chi_1(f(m,n)), & \text{如 }\chi\text{ 为 mod }p^{\alpha+1}\text{ 非原特征,}\end{cases}$$

在后一种情形下，χ_1 为一个 mod p^α 的非主特征，其定义见引理 1.22 的证明。于是由归纳假设，此时引理对 $\alpha+1$ 也成立。

总之，引理已被完全证明。

引理 1.25 设 α 为正整数，χ 为 mod 2^α 的非主特征，$f(x,y)=ax^2+bxy+cy^2$ 是判别式 $d=b^2-4ac$ 的二元二次原型。则有

$$\frac{1}{2^\alpha\varphi(2^\alpha)}\sum_{m,n(\text{mod }2^\alpha)}\chi(f(m,n))$$
$$=\begin{cases}\chi(a)\ (\text{或 }\chi(c)), & \text{如 }\chi\text{ 的导子}=2^\alpha=4\text{ 或 }8,\ 2^\alpha\mid d,\text{ 且 }\dfrac{d}{2^\alpha}\equiv 0\text{ 或 }\chi(-1)\ (\text{mod }4),\text{ 同时 }a\text{ 奇(或 }c\text{ 奇),还有下面的附加说明;}\\ 0, & \text{否则。}\end{cases}$$

并且在前一种情形下，还要求：对奇数 n，$\chi(n)=\left(\frac{-4}{n}\right)$，$\left(\frac{8}{n}\right)$ 或 $\left(\frac{-8}{n}\right)$ (均是 Kronecker 符号)。

证明 I 当 $\alpha=1$ 时，仅有主特征，没有可证的。

II $\alpha=2$ 时，非主特征 $\chi(1)=1$，$\chi(3)=-1$，χ 是判别式为 -4 时的 Kronecker 符号，分别处理。

II$_1$ a, c 中至少有一个奇数，不妨设 a 为奇数。此时

$$\chi(a)\sum_{m,n(\text{mod }4)}\chi(f(m,n))=\sum_{m,n(\text{mod }4)}\chi(m^2+bmn+acn^2).$$

再分为二个情况。

II$_{1.1}$ b 偶时，令 $b=2b_1$，b_1 整数，故 $d=4d_1$，$d_1=b_1^2-ac$。于是

$$\chi(a)\sum_{m,n(\text{mod }4)}\chi(f(m,n))=\sum_{m,n(\text{mod }4)}\chi(m^2-d_1n^2)$$
$$=4(1+\chi(-d_1)+\chi(1-d_1))$$

$$=\begin{cases}8, & 当\ d_1\equiv 0\ 或\ 3 \pmod 4;\\ 0, & 当\ d_1\equiv 1\ 或\ 2 \pmod 4.\end{cases}$$

Ⅱ$_{1.2}$　b 奇时，此时 $d\equiv 1 \pmod 4$，易得

$$\chi(a)\sum_{m,n(\bmod 4)}\chi(f(m,n))=\sum_{m,n(\bmod 4)}\chi\left(m^2+mn-\frac{d-1}{4}n^2\right)=0.$$

Ⅱ$_2$　a, c 均为偶数时，由 $g.c.d.(a,\ b,\ c)=1$ 知 b 为奇数，易知

$$\sum_{m,n(\bmod 4)}\chi(f(m,n))=2(\chi(a+c+b)+\chi(a+c+b+2))=0.$$

这样，$\alpha=2$ 时，引理成立。

Ⅲ$_1$　$\alpha=3$ 时，共有四个特征，即主特征；导子为 4 的特征，即 $\left(\frac{-4}{n}\right)$；导子为 8 的特征，即 $\left(\frac{8}{n}\right)$或$\left(\frac{-8}{n}\right)$(后三者均为 Kronecker 符号)，后三者是非主特征。设 χ 为后三者之一，分几种情况。

Ⅲ$_1$　a, c 中至少有一个奇数，不妨设 a 为奇数。

Ⅲ$_{1.1}$　b 偶，$b=2b_1$，b_1 整数，此时 $d=4d_1$，d_1 整数，$d_1=b_1^2-ac$。此时

$$\chi(a)\sum_{m,n(\bmod 8)}\chi(f(m,n))=\sum_{m,n(\bmod 8)}\chi(m^2+bmn+acn^2)$$

$$=\sum_{m,n(\bmod 8)}\chi(m^2-d_1n^2)$$

$$=4\sum_{n(\bmod 8)}\chi(1-d_1n^2)+2\sum_{n(\bmod 8)}\chi(-d_1n^2)$$

$$+2\sum_{n(\bmod 8)}\chi(4-d_1n^2)$$

$$=16\chi(1-d_1)+8+8\chi(1-d)+8\chi(-d_1)+8\chi(4-d_1)$$

$$=\begin{cases}32, & \begin{cases}当\ \chi=\left(\frac{-4}{*}\right)且\ d_1\equiv 0\ 或\ 3 \pmod 4;\\ 或\ \chi=\left(\frac{8}{*}\right)且\ d_1\equiv 0\ 或\ 2 \pmod 8;\\ 或\ \chi=\left(\frac{-8}{*}\right)且\ d_1\equiv 0\ 或\ 6 \pmod 8;\end{cases}\\ & \begin{cases}当\ \chi=\left(\frac{-4}{*}\right)且\ d_1\equiv 1\ 或\ 2 \pmod 4;\end{cases}\end{cases}$$

$$\left\{ 0, \quad \begin{cases} \text{或 } \chi=\left(\frac{8}{*}\right) \text{且 } d_1 \not\equiv 0,\ 2 \pmod 8; \\ \text{或 } \chi=\left(\frac{-8}{*}\right) \text{且 } d_1 \not\equiv 0,\ 6 \pmod 8. \end{cases} \right.$$

Ⅲ$_{1.2}$ b 奇，这时 $d\equiv 1 \pmod 4$。而有

$$\chi(a)\sum_{m,n(\bmod 8)}\chi(f(m,n))=\sum_{m,n(\bmod 8)}\chi(m^2+mn+acn^2)$$

$$=\sum_{\substack{m(\bmod 8)\\ 1\leqslant n\leqslant 4}}\chi(m^2+2mn+4acn^2)$$

$$+\sum_{\substack{m(\bmod 8)\\ 1\leqslant n\leqslant 4}}\chi(m^2+(2n-1)m+ac)$$

$$=\sum_{\substack{m(\bmod 8)\\ 1\leqslant n\leqslant 4}}\chi(m^2-dn^2)+4\sum_{m(\bmod 8)}\chi(m^2+m+ac)$$

$$=2\sum_{m(\bmod 8)}\chi(m^2-d)+\sum_{m(\bmod 8)}\chi^2(m)+\sum_{m(\bmod 8)}\chi(m^2-4d)$$

$$+8(\chi(ac)+\chi(2+ac)+\chi(4+ac)+\chi(6+ac))$$

$$=4(\chi(4-d)+\chi(-d))+4+4\chi(1-4d)+0=0,$$

这是因为当 $\chi=\left(\frac{-4}{*}\right)$时，由 $d\equiv 1 \pmod 4$，即知前4个的和为 $4(-1-1+1+1)=0$。当 $\chi=\left(\frac{\pm 8}{*}\right)$ 时，$\chi(4+n)=-\chi(n)$，又 $1-4d\equiv 5 \pmod 8$，故得所需。

Ⅲ$_2$ 当 a, c 均为偶数时，此时由 $g.c.d.(a,\ b,\ c)=1$ 知 b 奇，故 $d\equiv 1 \pmod 8$。于是

$$\sum_{m,n(\bmod 8)}\chi(am^2+bmn+cn^2)=\sum_{\substack{m,n(\bmod 8)\\ m,n\text{奇}}}\chi(a+c+bmn)$$

$$=4\sum_{m(\bmod 8)}\chi(a+c+m)=0.$$

这样，$\alpha=3$ 时，引理也成立。

Ⅳ $\alpha\geqslant 4$ 时，由本小节开头所述，可知这时 mod 2^α 的特征如下所述：对一个奇数 n，存在整数 $\lambda\geqslant 0$，使

$$n\equiv(-1)^{\frac{1}{2}(n-1)}5^\lambda \pmod{2^\alpha},$$

mod 2^α 的 $\varphi(2^\alpha)$ 个特征可表为

$$\chi_{\mu,\nu}(n)=(-1)^{\frac{1}{2}(n-1)\mu}e^{2\pi i\nu\lambda/2^{\alpha-2}},\ \mu \bmod 2,\ \nu \bmod 2^{\alpha-2}.$$

$\chi_{\mu,\nu}$ 为主特征$\Longleftrightarrow 2|\mu$ 且 $2^{\alpha-2}|\nu$;

$\chi_{\mu,\nu}$ 为 mod 2^α 原特征$\Longleftrightarrow 2\nmid\nu$.

Ⅳ$_1$　a, c 中至少有一个奇数，不妨设 a 奇，于是

$$\chi(a)\sum_{m,n(\bmod 2^\alpha)}\chi(f(m,n))=\sum_{m,n(\bmod 2^\alpha)}\chi(m^2+bmn+acn^2).$$

Ⅳ$_{11}$　b 偶时，$b=2b_1$, b_1 为整数，此时上式等于

$$\sum_{m,n(\bmod 2^\alpha)}\chi(m^2-d_1n^2),$$

其中 $d_1=\dfrac{d}{4}=b_1^2-ac$.

下面再分别讨论 χ 是 mod 2^α 原特征和非原特征的情况。先看 χ 为 mod 2^α 原特征时的情况，这时 Gauss 和 $\tau(\bar{\chi})\neq 0$, 故有

$$\chi(m)=\frac{1}{\tau(\bar{\chi})}\sum_{u(\bmod 2^\alpha)}\bar{\chi}(u)e^{2\pi ium/2^\alpha},$$

于是

$$\begin{aligned}&\sum_{m,n(\bmod 2^\alpha)}\chi(m^2-d_1n^2)\\&=\frac{1}{\tau(\bar{\chi})}\sum_{u(\bmod 2^\alpha)}\bar{\chi}(u)\sum_{m(\bmod 2^\alpha)}e^{2\pi ium^2/2^\alpha}\sum_{n(\bmod 2^\alpha)}e^{-2\pi iud_1n^2/2^\alpha}\\&=\frac{1}{\tau(\bar{\chi})}\sum_{\substack{u(\bmod 2^\alpha)\\ u\text{奇}}}\bar{\chi}(u)\cdot\begin{Bmatrix}(1+i^u)2^{\frac{\alpha}{2}}, & \text{若 } 2|\alpha;\\ e^{\frac{\pi i}{4}u}2^{\frac{\alpha+1}{2}}, & \text{若 } 2\nmid\alpha.\end{Bmatrix}\\&\cdot\begin{Bmatrix}2^\alpha & ,\text{ 若 } \alpha_0\geqslant\alpha;\\ 0 & ,\text{ 若 } \alpha_0=\alpha-1;\\ (1+i^{-ud_0})2^{\frac{\alpha+\alpha_0}{2}} & ,\text{ 若 } \alpha-\alpha_0 \text{ 偶，且 } \geqslant 2;\\ e^{-\frac{\pi i}{4}ud_0}2^{\frac{\alpha+\alpha_0-1}{2}} & ,\text{ 若 } \alpha-\alpha_0 \text{ 奇，且 } \geqslant 3.\end{Bmatrix},\end{aligned}\tag{2.60}$$

这里已设 $d_1=d_02^{\alpha_0}$, $2\nmid d_0$, $\alpha_0\geqslant 0$, 上面用到的 Gauss 三角和的公式可参考华罗庚著《数论导引》p.183. 我们再分几种情况来考察上面的公式(2.60).

(a) $\alpha_0\geqslant\alpha$, 这时(2.60)右边的和，当 α 偶时，是

$$2^{\frac{3}{2}\alpha}\Big(\sum_{u(\bmod 2^\alpha)}\bar{\chi}(u)+\sum_{u(\bmod 2^\alpha)}\bar{\chi}(u)e^{2\pi iu2^{\alpha-2}/2^\alpha}\Big)=0,$$

这里用到 $\bar{\chi}$ 是 mod 2^α 原特征，且 $\alpha\geqslant 4$; 而当 α 奇时，是

$$2^{\frac{3\alpha+1}{2}}\Big(\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)e^{2\pi i u\cdot 2^{\alpha-3}/2^{\alpha}}\Big)=0,$$

这里也用到 $\bar{\chi}$ 是 mod 2^{α} 的原特征，且奇数 $\alpha\geqslant 4$，故 $\alpha\geqslant 5$。这些事实可参考华罗庚著《数论导引》p.175.

(b) $\alpha_0=\alpha-1$ 时，(2.60)的右边显然是零。

(c) $\alpha-\alpha_0$ 偶且 $\geqslant 2$，这时用与(a)相同的理由可知，(2.60)右边的和，当 α 偶时，是

$$2^{\alpha+\frac{\alpha_0}{2}}\sum_{\substack{u(\bmod 2^{\alpha})\\ u奇}}\bar{\chi}(u)(1+i^{u})(1+i^{-ud_0})$$

$$=2^{\alpha+\frac{\alpha_0}{2}}\Big(\big(1+(-1)^{\frac{1-d_0}{2}}\big)\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)$$

$$+\big(1+(-1)^{\frac{1+d_0}{2}}\big)\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)e^{2\pi i u 2^{\alpha-2}/2^{\alpha}}\Big)=0;$$

而当 α 奇时，是

$$2^{\alpha+\frac{1+\alpha_0}{2}}\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)e^{\frac{\pi i u}{4}}(1+i^{-ud_0})$$

$$=2^{\alpha+\frac{1+\alpha_0}{2}}\Big(\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)e^{2\pi i u 2^{\alpha-3}/2^{\alpha}}$$

$$+\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)e^{2\pi i(1-2d_0)u2^{\alpha-3}/2^{\alpha}}\Big)=0.$$

(d) $\alpha-\alpha_0$ 奇且 $\geqslant 3$，同理，(2.60)右边的和，当 α 偶时是

$$2^{\alpha+\frac{\alpha_0-1}{2}}\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)(1+i^{u})e^{-\frac{\pi i}{4}ud_0}$$

$$=2^{\alpha+\frac{\alpha_0-1}{2}}\Big(\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)e^{2\pi i u(-d_0)2^{\alpha-3}/2^{\alpha}}$$

$$+\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)e^{2\pi i u(2-d_0)2^{\alpha-3}/2^{\alpha}}\Big)=0;$$

而当 α 奇时，是

$$2^{\alpha+\frac{\alpha_0}{2}}\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)e^{\frac{\pi i u}{4}}e^{-\frac{\pi i}{4}ud_0}$$

$$=2^{\alpha+\frac{\alpha_0}{2}}\sum_{u(\bmod 2^{\alpha})}\bar{\chi}(u)e^{2\pi i u(1-d_0)2^{\alpha-3}/2^{\alpha}}=0.$$

总之，我们证明了，当 χ 为 mod 2^{α} 的原特征且 $\alpha\geqslant 4$ 时

$$\sum_{m,n(\bmod 2^{\alpha})}\chi(m^2-d_1n^2)=0.$$

以下再看 χ 不是 mod 2^α 原特征的情况。令 χ 的导子为 $2^{\alpha-s}$，则 $s\geqslant 1$。又因 χ 不是主特征，故 $\alpha-s\geqslant 2$。即有 $1\leqslant s\leqslant \alpha-2$。这样存在一个 mod $2^{\alpha-s}$ 的原特征 χ_1 使

$$\chi(n)=\chi_1(n)，\text{如} 2\nmid n.$$

命

$$m=2^{\alpha-s}m_1+m_2,\ n=2^{\alpha-s}n_1+n_2,$$
$$m_1,\ n_1(\bmod 2^s),\ 1\leqslant m_2,\ n_2\leqslant 2^{\alpha-s}.$$

则有

$$\sum_{m,n(\bmod 2^\alpha)}\chi(m^2-d_1n^2)=\sum_{\substack{1\leqslant m_2,n_2\leqslant 2^{\alpha-s}\\ m_1,n_1(\bmod 2^s)}}\chi_1(m_2^2-d_1n_2^2)$$
$$=4^s\sum_{1\leqslant m,n\leqslant 2^{\alpha-s}}\chi_1(m^2-d_1n^2). \qquad (2.61)$$

仍分几种情况来讨论。

(a) 当 $\alpha-s=2$ 时，用 Ⅱ 中已证明的结果可由(2.61)知，

$$\sum_{m,n(\bmod 2^\alpha)}\chi(m^2-d_1n^2)=4^s\sum_{m,n(\bmod 2^{\alpha-s})}\chi_1(m^2-d_1n^2)$$
$$=\begin{cases}2^{2\alpha-1}, & \text{如 } d_1\equiv 0 \text{ 或 } 3(\bmod 4);\\ 0, & \text{否则。}\end{cases}$$

(b) 当 $\alpha-s=3$ 时，用 Ⅱ 中已证明的结果可由(2.61)知

$$\sum_{m,n(\bmod 2^\alpha)}\chi(m^2-d_1n^2)=4^s\sum_{m,n(\bmod 2^{\alpha-s})}\chi_1(m^2-d_1n^2)$$
$$=\begin{cases}2^{2\alpha-1}, & \text{如 } d_1\equiv 0 \text{ 或 } 2\chi_1(-1)(\bmod 8);\\ 0, & \text{否则。}\end{cases}$$

我们指出 $\chi_1(-1)=\chi(-1)$。

(c) 当 $\alpha-s\geqslant 4$ 时，再用上述对 $\alpha\geqslant 4$ 的 mod 2^α 原特征已证明的事实可知，这时

$$\sum_{m,n(\bmod 2^\alpha)}\chi(m^2-d_1n^2)=4^s\sum_{m,n(\bmod 2^{\alpha-s})}\chi_1(m^2-d_1n^2)=0.$$

综上所述，当 $\alpha\geqslant 4$，a 奇，b 偶时，引理已明。

Ⅳ$_{12}$　当 b 奇时，这时 $d\equiv 1(\bmod 4)$，并有

$$\chi(a)\sum_{m,n(\bmod 2^\alpha)}\chi(f(m,n))$$
$$=\chi(b^2)\sum_{m,n(\bmod 2^\alpha)}\chi(m^2+mn+b_1n^2),$$

这里 b_1 是满足 $b^2b_1 \equiv ac \pmod{2^\alpha}$ 的整数。

当 χ 为 mod 2^α 的原特征时，命

$$m = 2^{\alpha-1}m_1 + m_2,\ n = 2^{\alpha-1}n_1 + n_2,$$
$$m_1,\ n_1 \pmod 2,\ 1 \leqslant m_2,\ n_2 \leqslant 2^{\alpha-1},$$

则有

$$\sum_{m,n \pmod{2^\alpha}} \chi(m^2 + mn + b_1n^2)$$
$$= \sum_{1 \leqslant m_2, n_2 \leqslant 2^{\alpha-1}} \sum_{m_1, n_1 \pmod 2} \chi(m_2^2 + m_2n_2 + b_1n_2^2 + 2^{\alpha-1}(m_1n_2 + m_2n_1))$$
$$= \frac{1}{\tau(\bar{\chi})} \sum_{1 \leqslant m_2, n_2 \leqslant 2^{\alpha-1}} \sum_{\substack{u \pmod{2^\alpha} \\ u\text{奇}}} \bar{\chi}(u) e^{2\pi i u(m_2^2 + m_2n_2 + b_1n_2^2)/2^\alpha} \cdot$$
$$\sum_{m_1 \pmod 2} (-1)^{m_1n_2} \cdot \sum_{n_1 \pmod 2} (-1)^{m_2n_1}$$
$$= \frac{4}{\tau(\bar{\chi})} \sum_{1 \leqslant m, n \leqslant 2^{\alpha-2}} \sum_{u \pmod{2^\alpha}} \bar{\chi}(u) e^{2\pi i 4u(m^2 + mn + b_1n^2)/2^\alpha} = 0. \tag{2.62}$$

附注 上式对任一个 mod 2^α 的原特征 χ 成立，只要 $\alpha \geqslant 2$。

当 χ 的导子为 $2^{\alpha-s}$，$1 \leqslant s \leqslant \alpha - 2$ 时，命 χ_1 为 mod $2^{\alpha-s}$ 的原特征，便有

$$\chi(n) = \chi_1(n),\ \text{如}\ n\ \text{奇}.$$

再命

$$m = 2^{\alpha-s}m_1 + m_2,\ n = 2^{\alpha-s}n_1 + n_2,$$
$$m_1,\ n_1 \pmod{2^s},\ 1 \leqslant m_2,\ n_2 \leqslant 2^{\alpha-s},$$

则有

$$\sum_{m,n \pmod{2^\alpha}} \chi(m^2 + mn + b_1n^2)$$
$$= 4^s \sum_{m,n \bmod 2^{\alpha-s}} \chi_1(m^2 + mn + b_1n^2) = 0,$$

这里用到(2.62)及其附注，这样，a，b 均奇时，引理已明。

N_2 a，c 均为偶数时，由 $g.c.d.(a, b, c) = 1$ 知 b 奇，且 $d \equiv 1 \pmod 8$。命

$$m = 2^{\alpha-1}m_1 + m_2,\ n = 2^{\alpha-1}n_1 + n_2,\ m_1,\ n_1 \pmod 2,$$
$$1 \leqslant m_2,\ n_2 \leqslant 2^{\alpha-1}.$$

即有

$$\sum_{m,n(\mathrm{mod}\ 2^\alpha)}\chi(f(m,n))$$
$$=\sum_{1\leqslant m_2,n_2\leqslant 2^{\alpha-1}}\ \sum_{m_1,n_1(\mathrm{mod}\ 2)}\chi(f(m_2,n_2)+b2^{\alpha-1}(m_1n_2+m_2n_1)),$$

于是可以仿照上述Ⅳ$_{12}$的方法,可以证明

$$\sum_{m,n(\mathrm{mod}\ 2^\alpha)}\chi(f(m,n))=0.$$

综合上面Ⅰ～Ⅳ,即知引理已被完全证明。

引理 1.26 设p为素数,α为正整数,再设χ_0为mod p^α的主特征,$f(x,y)=ax^2+bxy+cy^2$是判别式$d=b^2-4ac$的二元二次原型,则有

$$\sum_{m,n(\mathrm{mod}\ p^\alpha)}\chi_0(f(m,n))=p^\alpha\varphi(p^\alpha)\left(1-\frac{1}{p}\left(\frac{d}{p}\right)\right),$$

这里$\left(\frac{d}{p}\right)$为Kronecker符号。

证明 我们考虑二元二次同余方程

$$f(x,y)\equiv 0(\mathrm{mod}\ p)$$

$x,y(\mathrm{mod}\ p^\alpha)$的解数$I_\alpha$。

命

$$x=x_1+x_2p,\ y=y_1+y_2p,$$
$$1\leqslant x_1,\ y_1\leqslant p,\ 1\leqslant x_2,\ y_2\leqslant p^{\alpha-1},$$

即不难证明

$$I_\alpha=p^{2\alpha-2}I_1.\tag{2.63}$$

因此只需求出I_1,即可算得I_α。易见

$$I_1=\frac{1}{p}\sum_{u(\mathrm{mod}\ p)}\ \sum_{m,n(\mathrm{mod}\ p)}e^{2\pi iuf(m,n)/p}$$
$$=p+\frac{1}{p}\sum_{u=1}^{p-1}\ \sum_{m,n(\mathrm{mod}\ p)}e^{2\pi i(uam^2+ubmn+ucn^2)/p}\tag{2.64}$$

分几种情况来讨论,以下总设$p\nmid u$。

(1) 当$p\nmid 2a$时,命整数a'满足$2aa'\equiv 1(\mathrm{mod}\ p)$。于是

$$\sum_{m,n(\mathrm{mod}\ p)}e^{2\pi i(uam^2+ubmn+ucn^2)/p}$$
$$=\sum_{m,n(\mathrm{mod}\ p)}e^{2\pi iua(m^2-a'^2dn^2)/p},\tag{2.65}$$

用Gauss三角和的值(见华罗庚著《数论导引》p.183), 即知

(2.65)右边

$$=\left(\frac{ua}{p}\right)\cdot\begin{cases}1, & \text{当 } p\equiv 1 \pmod 4\\ i, & \text{当 } p\equiv 3 \pmod 4\end{cases}\cdot\sqrt{p}$$

$$\cdot\begin{cases}\left(\dfrac{aua'^2d}{p}\right)\cdot\begin{cases}1, & \text{当 } p\equiv 1 \pmod 4\\ i, & \text{当 } p\equiv 3 \pmod 4\end{cases}\cdot\sqrt{p}, & \text{如 } p\nmid d\\ p, & \text{如 } p\mid d\end{cases}$$

(这里$\left(\frac{*}{p}\right)$是 mod p 的 Legendre 符号，以下相同。)

$$=\begin{cases}\left(\dfrac{d}{p}\right)p, & \text{当 } p\nmid d;\\ \left(\dfrac{au}{p}\right)\cdot\begin{cases}1, & \text{当 } p\equiv 1 \pmod 4\\ i, & \text{当 } p\equiv 3 \pmod 4\end{cases}\cdot p^{\frac{3}{2}}; & \text{当 } p\mid d.\end{cases}\tag{2.66}$$

从而由(2.64)、(2.65)和(2.66)即有

$$I_1=p+\frac{1}{p}\cdot\begin{cases}\left(\dfrac{d}{p}\right)p(p-1), & \text{当 } p\nmid d\\ 0, & \text{当 } p\mid d\end{cases}$$

$$=\begin{cases}p, & \text{当 } p\mid d;\\ 1, & \text{当 } p\nmid d,\text{ 且 } d \text{ 不是 mod } p \text{ 二次剩余时};\\ 2p-1, & \text{当 } p\nmid d,\text{ 且 } d \text{ 是 mod } p \text{ 二次剩余时},\end{cases}\tag{2.67}$$

附注　当 $p\nmid 2c$ 时，(2.67)仍成立。

(2) $2\neq p\mid a,\ c$ 时，此时 $p\nmid b$，故 $p\nmid d$，且$\left(\frac{d}{p}\right)=1$。这时有

$$I_1=2p-1.\tag{2.68}$$

(3) $p=2$ 时，由(2.64)有

$$I_1=2+\frac{1}{2}(1+(-1)^a+(-1)^c+(-1)^{a+b+c})$$

$$=\begin{cases}2, & \text{如 } 4\mid d;\\ 1, & \text{如 } d\equiv 5 \pmod 8);\\ 3, & \text{如 } d\equiv 1 \pmod 8).\end{cases}\tag{2.69}$$

这样由(2.63)、(2.67)、(2.68)和(2.69)即有

$$\sum_{m,n(\bmod p^\alpha)}\chi_0(f(m,n))=p^{2\alpha}-I_{p^\alpha}=p^{2\alpha}-p^{2\alpha-2}I_1$$

$$=\begin{cases} p^{2\alpha}-p^{2\alpha-2}\cdot\begin{Bmatrix} p\ , & \text{当 } p\mid d; \\ 1\ , & \text{当 } \left(\dfrac{d}{p}\right)=-1; \\ 2p-1, & \text{当 } \left(\dfrac{d}{p}\right)=1 \end{Bmatrix}, & \text{如 } p \text{ 奇;} \\ 2^{2\alpha}-2^{2\alpha-2}\cdot\begin{Bmatrix} 2, & \text{当 } 4\mid d; \\ 1, & \text{当 } d\equiv 5 \pmod 8; \\ 3, & \text{当 } d\equiv 1 \pmod 8) \end{Bmatrix}, & \text{如 } p=2 \end{cases}$$

$$=p^{2\alpha}-p^{2\alpha-2}\left(p+\left(\frac{d}{p}\right)(p-1)\right)$$

$$=p^{2\alpha}-p^{2\alpha-1}-\left(\frac{d}{p}\right)p^{2\alpha-2}(p-1)$$

$$=p^{\alpha}\varphi(p^{\alpha})\left(1-\frac{1}{p}\left(\frac{d}{p}\right)\right),$$

这里$\left(\dfrac{d}{p}\right)$是 Kronecker 符号。引理证毕。

定理 1.8 的证明 注意定理中等式两边均为k的积性函数，故可以只对k为素数幂的情况加以证明即可，这正是上述三个引理，即引理 1.24、引理 1.25 和引理 1.26 的内容。所以我们的定理 1.8 终于得证。

推论 设f是一个判别式d为基本判别式的二元二次原型，再设k也是一个基本判别式，$\chi(*)=\left(\dfrac{k}{*}\right)$是 Kronecker 符号，则有

$$\frac{1}{|k|\varphi(|k|)}\sum_{m,n(\bmod |k|)}\chi(f(m,n))$$
$$=\begin{cases}\chi(f), & \text{如 } \chi \text{ 是 } \mathscr{C}(d) \text{ 的一个 genus 特征;} \\ 0\ , & \text{否则,}\end{cases}$$

这里$\mathscr{C}(d)$是判别式为d的二元二次原型类群($d<0$时，只考虑正定型)。

1.7 二次同余方程和二元二次型表整数

引理 1.27 设d为一个基本判别式，即$d(\neq 1)$为一个整数，

$d=d_0d_1$，其中 d_1 是一个无平方因子整数，并满足 $d_1\equiv 1 \pmod 4$，而整数 $d_0=1$，-4 或 ± 8。再设 n 是一个正整数。则同余方程

$$x^2\equiv d \pmod{4n} \tag{2.70}$$

$\chi \bmod 4n$ 的解数为

$$f(d,\ 4n)=\begin{cases}2\sum\limits_{1\leqslant m\mid n}\left(\dfrac{d}{m}\right)\left|\mu(m)\right|, & \text{如 } p\mid d\Longrightarrow p^2\nmid n;\\ 0 & \text{，否则，}\end{cases}$$

这里$\left(\dfrac{d}{*}\right)$是 Kronecker 符号，$\mu(*)$为 μöbius 函数，$p$ 表素数。

附注 (1) 可知，同余方程 (2.70)，$x \bmod 2n$ 的解数是 $\dfrac{1}{2}f(d,\ 4n)$。

(2) 当 $g.c.d.(d,\ n)=1$ 时，本引理对一般的判别式也成立即知此时(2.70) $x \bmod 4n$ 的解数是

$$2\sum_{1\leqslant m\mid n}\left(\frac{d}{m}\right)\left|\mu(m)\right|,$$

而此时(2.70) $x \bmod 2n$ 的解数是

$$\sum_{1\leqslant m\mid n}\left(\frac{d}{m}\right)\left|\mu(m)\right|.$$

这可见之于华罗庚著《数论导引》p.340 定理 12.3.4.。

证明 这可由第一章的引理 2.13 直接得出。

引理 1.28 设 d 为基本判别式，k 为正整数，$F_r(x,\ y)$ $(1\leqslant r\leqslant H)$是判别式为 d 的二元二次型类群的完全代表元组，以 $\psi_0(k)$ 记以下 H 个不定方程

$$F_1(x,\ y)=k,\ \cdots,\ F_H(x,\ y)=k$$

的原解(定义见第一章 §2.2)总数。则有

$$\psi_0(k)=w\sum_{1\leqslant m\mid k}\left(\frac{d}{m}\right),$$

这里$\left(\dfrac{d}{*}\right)$ 是 Kronecker 符号，$w=1,\ 2,\ 4,\ 6$ 视 $d>0$，$d<-4$，$d=-4$，$d=-3$ 而定。注意 $d<0$ 时，只考虑正定型。

证明 先从同余方程

$$l^2 \equiv d \pmod{4k},\ 0 \leqslant l < 2k \tag{2.71}$$

的解说起。对(2.71)的一个解l，由$l^2-4km=d$可定出一个整数m。这样就得到一个判别式为d的二元二次型$((k, l, m))$（由于d是基本判别式，故它是原型），它必与$F_r(1\leqslant r\leqslant H)$之中的一个相似且正好与一个相似。又由第一章§2.2知，对每一个l有w个既约原解，所以由引理1.27的附注(1)即知

$$F_1(x, y)=k, \cdots, F_H(x, y)=k$$

的既约原解的总数为

$$w\sum_{1\leqslant m|k}\left(\frac{d}{m}\right)|\mu(m)|.$$

从而原解总数为

$$\begin{aligned}\psi_0(k) &= w\sum_{\substack{n^2|k\\ n\geqslant 1}}\ \sum_{1\leqslant m\left|\frac{k}{n^2}\right.}\left(\frac{d}{m}\right)|\mu(m)|\\ &= w\sum_{\substack{mn^2|k\\ m,n\geqslant 1}}\left(\frac{d}{m}\right)|\mu(m)| = w\sum_{1\leqslant m|k}\left(\frac{d}{m}\right),\end{aligned}$$

最后一个等式的成立的证明，因两边的和均为k的积性函数，然后对k为素数幂的情况加以验证即可。引理证毕。

附注　引理1.28对一般的判别式d，在满足条件g.c.d.$(k, d)=1$时，仍然成立，见华罗庚著《数论导引》p.342.定理12.4.1.。

1.8　二元二次型类群的解析类数公式

设d为一个判别式，$\chi(*)$为Kronecker符号$\left(\frac{d}{*}\right)$。令

$$L(s, \chi)=\sum^{\infty}\frac{\chi(n)}{n^s},\ s=\sigma+\mathrm{i}t,\ \sigma=\mathrm{Re}\, s>1.$$

则$L(s, \chi)$是在$\mathrm{Re}\, s>1$半平面中的解析函数，它可开拓为整个s平面上的整函数，并有

$$L(1, \chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n}.$$

那么我们有下面的类数公式。

定理1.9　对判别式为d的二元二次原型类群$\mathscr{C}(d)$，其类

数

$$H_0(d)=\begin{cases}\dfrac{w\sqrt{|d|}}{2\pi}L(1,\ \chi),\ \text{如}\ d<0;\\[2ex] \dfrac{\sqrt{d}}{\log\varepsilon_+}L(1,\ \chi),\quad \text{如}\ d>0,\end{cases}$$

这里 $w=2,\ 4,\ 6$ 视 $d<-4,\ d=-4,\ d=-3$ 而定；而当 $d>0$ 时，ε_+ 是 Pell 方程

$$x^2-dy^2=4$$

的基本解(即最小解)；$L(1,\ \chi)$ 如上所示。

证明 见华罗庚著《数论导引》第十二章。

每一个判别式 d 都可唯一地表达为下列形状：

$$d=d_0d_1^2, \tag{2.72}$$

其中 d_0 为一个基本判别式，而 d_1 为一个正整数。

引理 1.29 对一个判别式 d，在分解式(2.72)之下，有

$$\frac{H_0(d)}{H_0(d_0)}=\frac{d_1}{w_1}\prod_{p\mid d_1}\left(1-\frac{1}{p}\left(\frac{d_0}{p}\right)\right),$$

这里 $H_0(d)$ 与 $H_0(d_0)$ 分别表示判别式为 d 与 d_0 的二元二次原型类群 $\mathscr{C}(d)$ 与 $\mathscr{C}(d_0)$ 的类数；对 $d<0$，

$$w_1=\begin{cases}1,\ \text{如}\ d_0<-4;\ \text{或}\ d_0=-4,\ -3,\ \text{而}\ d_1=1;\\ 2,\ \text{如}\ d_0=-4,\ \text{而}\ d_1>1;\\ 3,\ \text{如}\ d_0=-3,\ \text{而}\ d_1>1.\end{cases}$$

而对 $d>0$，w_1 如下定义之：Pell 方程

$$x^2-dy^2=4$$

的基本解 ε_d 是 Pell 方程

$$x^2-d_0y^2=4$$

的基本解 ε_{d_0} 的一个正整数次幂 $\varepsilon_{d_0}^{w_1}$，即有

$$w_1=\frac{\log\varepsilon_d}{\log\varepsilon_{d_0}},$$

也可记为

$$w_1=J(d;\ d_0),$$

这后一记号，将可见之于第7章；最后$\left(\frac{d_0}{*}\right)$是 Kronecker 符号。

证明 经简单计算即得。

引理 1.30 设以 $H_0(d_0)$ 与 $H_0(d)$ 分别记判别式为 d_0 与 d 的二元二次原型类群 $\mathscr{C}(d_0)$ 与 $\mathscr{C}(d)$ 的类数，且分解式(2.72)成立。则我们有

$$H_0(d_0) \mid H_0(d).$$

证明 由引理 1.29 知，只需证明

$$w_1 \left| d_1 \prod_{p \mid d_1}\left(1-\frac{1}{p}\left(\frac{d_0}{p}\right)\right)\right., \tag{2.73}$$

其中$\left(\frac{d_0}{p}\right)$为 Kronecker 符号，当 $d<0$ 时，(2.73)容易验证。而当 $d>0$ 时，(2.73)的证明即是应证明

$$J(d; d_0) \left| d_1 \prod_{p \mid d_1}\left(1-\frac{1}{p}\left(\frac{d_0}{p}\right)\right)\right., \text{ 如 } d>0, \tag{2.74}$$

其中$\left(\frac{d_0}{p}\right)$为 Kronecker 符号。

命$\varepsilon_0=\varepsilon_{d_0}=\frac{a_1+b_1\sqrt{d_0}}{2}$为 Pell 方程

$$x^2-d_0y^2=4$$

的基本解。(2.74)等价于

$$d_1 \mid b_n,\ n=d_1 \prod_{p \mid d_1}\left(1-\frac{1}{p}\left(\frac{d_0}{p}\right)\right), \tag{2.75}$$

其中由

$$\left(\frac{a_1+b_1\sqrt{d_0}}{2}\right)^n=\frac{a_n+b_n\sqrt{d_0}}{2}$$

决定 b_n。

易见只需对 d_1 为素数幂时证明(2.75)。令 $d_1=p^s$，p 为素数，整数 $s\geqslant 1$。又 $p \mid d_0$ 时，(2.75)显然成立。故可设 $p \nmid d_0$。先看 $s=1$ 的情形。

(1) $p=2$ 时，这时

$$n=2-\left(\frac{d_0}{2}\right)=\begin{cases}1, & \text{如 } d_0\equiv 1 \pmod 8;\\ 3, & \text{如 } d_0\equiv 5 \pmod 8.\end{cases}$$

b_1偶时，(2.75)显然成立，故可设 b_1 为奇数，这时由 $a_1^2-b_1^2d_0=4$ 即知有 $a_1^2\equiv 4+d_0 \pmod 8$，故可得

$$d_0\equiv 5 \pmod 8,\ a_1\ \text{奇},\ n=3,\ b_3=(a_1^2-1)b_1.$$

于是(2.75)仍成立。这样 $s=1$，$p=2$ 时，(2.75)成立。

(2) p奇时，$n=p-\left(\frac{d_0}{p}\right)$（$\left(\frac{d_0}{p}\right)$ Legendre 符号）。$p\mid b_1$ 时，(2.75)显然成立。故可设 $p\nmid b_1$，对任一个正整数 m，有

$$b_m=2^{-m+1}\sum_{\substack{1\le t\le m\\ t\ \text{奇}}}\binom{m}{t}a_1^{m-t}b_1^t d_0^{\frac{t-1}{2}},\tag{2.76}$$

这里$\binom{m}{t}$为二项展开式系数，特别有（注意 $p\nmid 2d_0$）

$$2^{p-1}b_p\equiv b_1^p d_0^{\frac{p-1}{2}} \pmod p,$$

从而有

$$b_p\equiv b_1\left(\frac{d_0}{p}\right) \pmod p\tag{2.77}$$

又由(2.76)有

$$2^p b_{p+1}\equiv (p+1)a_1^p b_1+(p+1)a_1 b_1^p d_0^{\frac{p-1}{2}} \pmod p,$$

从而

$$2b_{p+1}\equiv a_1b_1+a_1b_1\left(\frac{d_0}{p}\right) \pmod p\tag{2.78}$$

因此当$\left(\frac{d_0}{p}\right)=-1$时，(2.75)已成立。如$\left(\frac{d_0}{p}\right)=1$，则由(2.77)、(2.78)有

$$b_{p+1}\equiv a_1b_1 \pmod p,\ b_p\equiv b_1 \pmod p.\tag{2.79}$$

由 b_n 的定义可得

$$b_{p+1}=a_1b_p-b_{p-1}\tag{2.80}$$

（这可如下得出：ε_0 满足二次方程

$$x^2-a_1x+1=0,$$

故有

$$\varepsilon_0^{n+1}-a_1\varepsilon_0^n+\varepsilon_0^{n-1}=0,\ n\geqslant 1.$$

由此即得(2.80))。

于是由(2.79)和(2.80)即得

$$b_{p-1}\equiv 0(\bmod\ p).$$

即$\left(\frac{d_0}{p}\right)=1$ 时，(2.75)仍成立。

总之，我们已证明了，对任一个素数 p 有

$$b_{p-\left(\frac{d_0}{p}\right)}\equiv 0(\bmod\ p),$$

这里$\left(\frac{d_0}{p}\right)$是 Kronecker 符号，由此对 s 用归纳法，即得

$$b_{p^{s-1}\left(p-\left(\frac{d_0}{p}\right)\right)}\equiv 0(\bmod p^s).$$

这就给出了所需要证明的事实，同时也就完成了引理的证明。

附注 由上述证明可见，下断断言成立。

断言 设 d_0 为一个判别式，$d_0>0$，d_1 为一个正整数，而 $J(d_0d_1^2; d_0)$的定义如上所述，则有：

$$J(d_0d_1^2;d_0)\mid d_1\prod_{p\mid d_1}\left(1-\frac{1}{p}\left(\frac{d_0}{p}\right)\right),$$

这里$\left(\frac{d_0}{p}\right)$是 Kronecker 符号。

这个断言有独立的兴趣。

定理 1.10 判别式为 d 的二元二次原型广义相似类群的类数

$$h_0(d)=\begin{cases}\dfrac{w\sqrt{|d|}}{2\pi}L(1,\chi), & \text{如 } d<0;\\[2mm] \dfrac{\sqrt{d}}{2\log\varepsilon}L(1,\chi), & \text{如 } d>0,\end{cases}$$

这里对 $d<0$，$w=2,4,6$ 视 $d<-4$，$d=-4$，$d=-3$ 而定；当 $d>0$ 时，ε 是广义 Pell 方程

$$x^2-dy^2=\pm 4$$

的基本解，最后

$$L(1,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n},$$

其中 $\chi(*)=\left(\frac{d}{*}\right)$是 Kronecker 符号。

证明　由定义、定理1.9、第一章§2.1以及本章的引理1.3可得本定理的证明。

引理1.31　设判别式 $d=d_0d_1^2$，其中 d_0 为基本判别式，则

$$h_0(d_0)\mid h_0(d).$$

证明　$d<0$ 时，$h_0=H_0$，故由引理1.30即得所需。

当 $d_0>0$，$N(\varepsilon_0)=1$ 时，这里 ε_0 为广义 Pell 方程

$$x^2-d_0y^2=\pm 4$$

的基本解，即 $x^2-d_0y^2=-4$ 无解，则也有 $N(\varepsilon_d)=1$，这里 ε_d 是广义 Pell 方程

$$x^2-dy^2=\pm 4$$

的基本解，即 $x^2-dy^2=-4$ 也无解。那么

$$h_0(d_0)=\frac{1}{2}H_0(d_0),\ h_0(d)=\frac{1}{2}H_0(d),$$

由此及引理1.30也得所需。

当 $d_0>0$，$N(\varepsilon_0)=-1$ 时，$h_0(d_0)=H_0(d_0)$，但是 $h_0(d)=\frac{1}{2}H_0(d)$或 $H_0(d)$，视 $N(\varepsilon_d)=1$ 或 -1 而定，无论怎样，$h_0(d_0)\mid 2h_0(d)$ 总是成立的。因此为证明我们的引理，只需对 $d_0>0$，

$$x^2-d_0y^2=-4,$$

有解，而

$$x^2-d_0d_1^2y^2=-4$$

无解的情形，证明

$$2J(d_0d_1^2;d_0)\,\Big|\,d_1\prod_{p\mid d_1}\left(1-\frac{1}{p}\left(\frac{d_0}{p}\right)\right) \tag{2·81}$$

即可，其中 $\left(\frac{d_0}{p}\right)$ 为 Kronecker 符号。

命 $x^2-d_0y^2=-4$ 的基本解为 $\varepsilon_-=\frac{a_1+b_1\sqrt{d_0}}{2}$，则 $x^2-d_0y^2=4$ 的基本解为 $\varepsilon_+=\varepsilon_-^2=\frac{a_2+b_2\sqrt{d_0}}{2}$，其中 $a_2=a_1^2+2$，$b_2=a_1b_1$.

如存在 d_1 的一个奇素因子 $p\nmid d_0$，则仿引理1.30的证明可知，

$$b_{p-\left(\frac{d_0}{p}\right)}\equiv 0 \pmod p,$$

即有

$$J(d_0p^2; d_0)\left|\frac{1}{2}\left(p-\left(\frac{d_0}{p}\right)\right)\right..$$

由此即得(2.81)。因此可设 d_1 的每一个奇素因子均除尽 d_0。

又当 $2|d_1$ 时，如 d_0 偶，则有 $d_0\equiv 0 \pmod 4$，再由 $a_1^2-b_1^2d_0=-4$，即知 a_1 偶，从而 b_2 偶，这证明了 $J(4d_0; d_0)=1$，即知这时(2.81)成立；当 $d_0\equiv 1 \pmod 8$ 时，仍得 b_2 为偶数，同样可知(2.81)成立；当 $d_0\equiv 5 \pmod 8$ 时，由 $a_1^2-b_1^2d_0=-4$ 可知，a_1 与 b_1 同奇偶，如 a_1 与 b_1 同为偶数，则 b_2 为偶数，此时仍有(2.81)成立，而 a_1 与 b_1 同为奇数时，a_2，b_2 均是奇数，$b_4=a_2b_2$ 为奇数，$a_3=a_1(a_2+1)$ 与 $b_3=(a_1^2+1)b_1$ 同为偶数，即得 $b_6\equiv 0 \pmod 4$。于是 $J(16d_0; d_0)=3$，这样 $4|d_1$ 时，(2.81)仍然成立。这里 a_n，b_n 由 $\frac{a_n+b_n\sqrt{d_0}}{2}=\left(\frac{a_1+b_1\sqrt{d_0}}{2}\right)^n$ 决定。

总结上一段的说明，我们可设 $2\|d_1$，或 d_1 奇，d_1 的奇素因子均除尽 d_0，$d_0\equiv 5 \pmod 8$，且 a_1，b_1 同为奇数。令

$$d_1=d_1' \text{ 或 } 2d_1',$$

其 d_1' 为奇数，且 d_1' 的素因子均除尽 d_0。

当 $d_1=d_1'$ 时，对 d_1' 的素因子个数用归纳法，即知

$$x^2-d_0d_1^2y^2=-4$$

有解，这与假设矛盾。于是 $d_1=2d_1'$。如果

$$x^2-4d_0y^2=-4 \tag{2.82}$$

有解，则仿上对 d_1' 的素因子个数用归纳法，即知

$$x^2-d_0d_1^2y^2=-4$$

有解，从而与假设矛盾。但由 a_1，b_1 奇，可知 b_3 为偶数，这时(2.82)确实可解，由刚才的说明，这是不可能的。这样就完成了我们对引理的证明。

1.9 Gauss 类数猜想的提出

对给定的判别式 d, 决定二元二次原型类群 $\mathscr{C}(d)$ 的结构，当然可以由上述各小节中所阐述的理论一步一步地完成，对于较小的 d, Gauss 在其名著中确实做了这一工作。他特别发现了，就已算出的情况来看，$d<0$ 时，$H_0(d)=1$ 的 d 并不是很多。

由以上各小节的理论可知，我们只需对基本判别式 d 来考察广义相似类数 $h(d)$ 即可。注意对基本判别式，型与原型是一致的，故 $h_0=h$。下面如无特殊的声明，总设 d 是基本判别式。

又 $\mathscr{C}(d)$ 的族群的阶 $g(d)$，也是 $\mathscr{C}(d)$ 的 Ambiguous 子群 $\mathscr{A}(d)$ 的阶，所以 $g(d)\mid H(d)$。由定理 1.5 知

$$g(d)=2^{\lambda-1},$$

这里 λ 是基本判别式 d 所含的素因子的个数。

于是对负的基本判别式 $d<0$，由 $h(d)=H(d)$，即有 $2^{\lambda-1}\mid h(d)$，λ 是 d 所含素因子的个数，并且 $\frac{h(d)}{2^{\lambda-1}}$ 是 $\mathscr{C}(d)$ 的主族中所含的类的个数。这样，当且仅当 $d=-4$，-8 或 $-p$(素数 $p\equiv 3 \pmod 4$)时，$|\mathscr{A}(d)|=1$，并且只有这时 $h(d)$ 才可能是奇数。反之，如果这时有 $2\mid h(d)=H(d)$，则存在一个 $\mathfrak{A}\in\mathscr{C}(d)$，使 $\mathfrak{A}\neq[1]$，但 $\mathfrak{A}^2=[1]$，即 $\mathfrak{A}$ 是 $\mathscr{A}(d)$ 的一个非恒等元，与 $|\mathscr{A}(d)|=1$ 矛盾。从而这时 $h(d)$ 一定是奇数。所以得到下面的引理。

引理 1.32 当 d 为一个负的基本判别式，判别式为 d 的二元二次型的广义相似类群的阶 $h(d)$ 为奇数的充要条件是 $d=-4$，-8 或 $-p$，这儿素数 $p\equiv 3 \pmod 4$。

经计算，Gauss 得出：

$h(d)=1$，如 $d=-3$，-4，-7，-8，-11，-19，-43，-67，-163。

而再继续算下去，再也没有得到使 $h(d)=1$ 的负的基本判别式了，因此他提出了下列著名的 Gauss 猜想。

Gauss 猜想(I) 正好存在上述九个负的基本判别式 $d<0$，

使 $h(d)=1$。

引理 1.33 设判别式为 $d>0$(本引理中不要求 d 为基本判别式)的二元二次原型 $((a, b, c))\approx((-a, -b, -c))$。则存在整数 x, y, 使 $d=x^2+y^2$。

证明 不妨设有理整数 a, b, c 满足

$$|b|\leqslant a\leqslant c,\ g.c.d.(a, b, c)=1,\ d=b^2+4ac, \tag{2.83}$$

而有

$$f=((a, -b, -c))\approx((-a, b, c)), \tag{2.84}$$

并且

$$a=\min_{\substack{x,y\in\mathbb{Z}\\(x,y)\neq(0,0)}}|f(x, y)|. \tag{2.85}$$

由定义知,存在 $r, u, s, t\in\mathbb{Z}$ 使

$$ru-st=1. \tag{2.86}$$

$$-a=ar^2-brt-ct^2, \tag{2.87}$$

$$b=2ars-b(ru+st)-2ctu, \tag{2.88}$$

$$c=as^2-bsu-cu^2. \tag{2.89}$$

由(2.86)—(2.89),不难证明(用矩阵形式):

$$u=-r,\ as+br+ct=0,\ r^2+st=-1. \tag{2.90}$$

显然有 $ts\neq0$。如 $r=0$, 则有 $s=-t=\pm1$, 于是 $c=a$, 从而 $d=b^2+4ac=b^2+4a^2$, 引理的结论成立。因此不妨设

$$r,\ t>0,\ g.c.d.(r, t)=1, \tag{2.91}$$

最多只需把 b 改变一下符号。首先假定在 (2.83)—(2.91) 下有 $b\geqslant0$。

今由(2.83)与(2.85)知有

$$b\leqslant a=\min|f|<\frac{\sqrt{d}}{2},$$

从而由第一章的引理1.6、引理1.7与 (2.87) 可知 $\frac{r}{t}$ 是 $\alpha=\frac{b+\sqrt{d}}{2a}$ 的一个渐近分数 $\frac{p_{n-1}}{q_{n-1}}(n\geqslant1)$。

把 α 展开为简单连分数:

$$\alpha=[a_0, \overline{a_1, \cdots, a_k}],$$

这里$\overline{a_1, \cdots, a_k}$为基本周期，而$k$为周期长度。用第一章的记号，由(2.87)有

$$-a = ap_{n-1}^2 - bp_{n-1}q_{n-1} - cq_{n-1}^2 = (-1)^n Q_n. \qquad (2.92)$$

于是n为奇数，且

$$Q_n = a = Q_0 = Q_k. \qquad (2.93)$$

如$n=1$，则$p_0 = a_0$，$q_0 = 1$，且由(2.92)有

$$-a = aa_0^2 - ba_0 - c,$$

故得

$$c = a(a_0^2 + 1) - ba_0,\ d = b^2 + 4ac = (2aa_0 - b)^2 + 4a^2.$$

即引理的结论成立。故可设

$$n \geqslant 3,\ n \equiv 1 \pmod 2. \qquad (2.94)$$

由(2.90)及

$$r = p_{n-1},\ t = q_{n-1},\ p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = (-1)^{n-2} = -1 \qquad (2.95)$$

即知存在一个整数$w \geqslant 1$使

$$u = -p_{n-1} = -wq_{n-1} - q_{n-2},\ s = -wp_{n-1} - p_{n-2}. \qquad (2.96)$$

由(2.88)、(2.95)、(2.96)，经计算可得

$$\begin{aligned} b &= 2aw - (2ap_{n-1}p_{n-2} - b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) - 2cq_{n-1}q_{n-2}) \\ &= 2aw - P_n, \end{aligned}$$

最后一个等式用了第一章的有关结果(即(1.17))。于是有

$$P_n = 2aw - b \qquad (2.97)$$

由(2.93)及(2.97)即知，α的第n个完全商

$$\alpha_n = \frac{P_n + \sqrt{d}}{2Q_n} = \frac{2aw - b + \sqrt{d}}{2a} = w + \beta, \qquad (2.98)$$

这里$\beta = \dfrac{\sqrt{d} - b}{2a}$，$\beta$的简单连分数展开式可由$\alpha$来刻划，这已于第一章的引理1.5中阐明。由此用归纳法，由(2.98)可得

$$P_{n+j} = P_{n+1-j},\quad 如\ 1 \leqslant j \leqslant k, \qquad (2.99)$$

$$Q_{n+j} = Q_{n-j},\quad 如\ 1 \leqslant j \leqslant k, \qquad (2.100)$$

令

$$n = n_1 k + n_0,\ 1 \leqslant n_0 \leqslant k,\ n_1 \geqslant 0. \tag{2.101}$$

如 n_0 奇，且 $n_0 \geqslant 3$，则令 $n_0 = 2m_0 - 1$，$m_0 \geqslant 2$。则由(2.100)有

$$Q_{m_0-1} = Q_{k+m_0-1} = Q_{2m_0-1+k-m_0} = Q_{n+k-m_0} = Q_{m_0},$$

由此即知 $d = P_{m_0}^2 + 4Q_{m_0}Q_{m_0-1} = P_{m_0}^2 + 4Q_{m_0}^2$，即引理成立。

如 $n_0 = 1$，则由(2.93)有

$$Q_1 = Q_{n_0} = Q_n = a = Q_0,$$

故有 $d = P_1^2 + 4Q_1Q_0 = P_1^2 + 4Q_1^2$，因此引理仍成立。

如 n_0 为偶数，则由 n 奇，且 $n \geqslant 3$(即(2.94))，以及(2.101)知

$$k\ 为奇数,\ n_0 = 2m_0,\ m_0 \in \mathbb{Z}.\ 1 \leqslant m_0 \leqslant \frac{k-1}{2}.$$

取 $l = \frac{k-1}{2} - m_0$。如 $l \geqslant 1$，则由(2.100)可得

$$Q_{\frac{k-1}{2}+m_0} = Q_{2m_0+l} = Q_{n+l} = Q_{k-l} = Q_{\frac{k-1}{2}+m_0+1},$$

故 $d = P^2_{\frac{k-1}{2}+m_0+1} + 4Q^2_{\frac{k-1}{2}+m_0+1}$，因此引理成立。

如 $l = 0$，则 $2m_0 = k - 1$，由(2.93)有

$$Q_{k-1} = Q_{2m_0} = Q_n = Q_k.$$

故 $d = P_k^2 + 4Q_k^2$，即引理成立。

以上证明了在(2.83)—(2.91)下及 $b \geqslant 0$ 时，引理成立。现在假设在(2.83)—(2.91)下，有 $b < 0$。如果此时有

$$0 < \frac{\sqrt{d} - |b|}{2a} < 1,$$

则由第一章引理 1.5 即知

$$\alpha = \frac{|b| + \sqrt{d}}{2a}\ 的简单连分数展开式$$

$$\alpha = [a_0, \overline{a_1, \cdots, a_k}],\ \overline{a_1, \cdots, a_k}\ 是基本周期,$$

其中有

$$a_k - a_0 = 0, \tag{2.102}$$

又由第一章(1.38)有

$$a_k = 2a_0\ 或\ 2a_0 - 1. \tag{2.103}$$

再结合 $a_0 \geqslant 1$，由(2.102)与(2.103)即得

$$a_k=a_0=1. \tag{2.104}$$

由(2.85)即知也有

$$a=\min_{\substack{x,y\in\mathbf{Z}\\(x,y)\neq 0}}|ax^2-|b|xy-cy^2|. \tag{2.105}$$

于是由(2.104)和(2.105)，第一章的引理1.11及其证明之后的附注，即知

$$\alpha=\frac{|b|+\sqrt{d}}{2a}\sim\frac{1+\sqrt{5}}{2}.$$

从而有$a=|b|=c=1$，$d=5=1+2^2$，引理仍成立。

而$\dfrac{\sqrt{d}-|b|}{2a}>1$时，则可证明$\dfrac{r+t}{t}$是$\dfrac{\sqrt{d}-|b|}{2a}+1$的渐近分数，从而$\dfrac{r}{t}$是$\dfrac{\sqrt{d}-|b|}{2a}$的渐近分数，故可仿$b\geqslant 0$时同样证明引理。引理证毕。

对正的基本判别式$d>0$，欲$h(d)$为奇数，必需$|\mathscr{A}(d)|=1$或2。对两种情况分别讨论。

由定理1.5知，对正的基本判别式$d>0$，$|\mathscr{A}(d)|=1$，当且仅当$d=8$或$d=$素数$p\equiv 1\pmod 4$。易见此时有$N(\varepsilon)=-1$。于是$h(d)=H(d)$，从而此时$h(d)$为奇数。

同样，对正的基本判别式$d>0$，$|\mathscr{A}(d)|=2$当且仅当$d=4q$(素数$q\equiv 3\pmod 4$)，$8q$(素数$q\equiv 3\pmod 4$)，q_1q_2(素数q_1,q_2均$\equiv 3\pmod 4$，且$q_1\neq q_2$)，$8p$(素数$p\equiv 1\pmod 4$)，p_1p_2(素数p_1，p_2均$\equiv 1\pmod 4$，且$p_1\neq p_2$)。前三种情况下，均有$N(\varepsilon)=+1$，而在后二种情况下，$N(\varepsilon)=\pm 1$均是可能的。

先看前三种情况，这时$h(d)=\dfrac{1}{2}H(d)$。我们来证明在这三种情况下，$h(d)$必为奇数。用反证法，若$h(d)$为偶数，则$4|H(d)$。由于$\mathscr{C}(d)$的二阶元均在$\mathscr{A}(d)$中，所以$\mathscr{C}(d)$必含有一个四阶元$\mathfrak{A}=[((a,b,c))]$：

$$\mathfrak{A}^4=[1],\ [1]\neq\mathfrak{A}^2\in\mathscr{A}(d). \tag{2.106}$$

易见

$$\mathscr{A}(d)=\{[1],\ \mathfrak{B}\},\tag{2.107}$$

其中

$$\mathfrak{B}=\begin{cases}[((-1,\ 0,\ q))],\ 如\ d=4q,\ 素数\ q\equiv 3(\mathrm{mod}\ 4);\\ [((-1,\ 0,\ 2q))],\ 如\ d=8q,\ 素数\ q\equiv 3(\mathrm{mod}\ 4);\\ \left[\left(\left(-1,\ 1,\ \dfrac{q_1q_2-1}{4}\right)\right)\right],\ 如\ d=q_1q_2,\end{cases}\tag{2.108}$$

最后一种情况中，素数 q_1，q_2 均 $\equiv 3(\mathrm{mod}\ 4)$，且 $q_1\neq q_2$。

由(2.106)与(2.107)有 $\mathfrak{A}^2=\mathfrak{B}$，又 $\mathfrak{A}^{-1}=[((a,\ -b,\ c))]$，故不难证明在(2.108)这三种情况下，均有

$$\mathfrak{A}^{-1}\mathfrak{B}=[((-a,\ -b,\ -c))],\tag{2.109}$$

于是由

$$\mathfrak{A}=\mathfrak{A}^{-1}\mathfrak{B},$$

即得

$$((a,\ b,\ c))\approx((-a,\ -b,\ -c)).$$

这样，由引理 1.33，即知存在整数 x，y 使

$$x^2+y^2=d=4q,\ 8q,\ q_1q_2,$$

由于 q，q_1，$q_2\equiv 3\ (\mathrm{mod}\ 4)$，这是不可能的。这就证明了 $h(d)$ 是奇数。

对后二种情况，我们来证明 $h(d)$ 是偶数。当 $N(\varepsilon)=-1$ 时，$h(d)=H(d)$，又 $2=|\mathscr{A}(d)|$ 是 $H(d)$ 的因子，因此可设 $N(\varepsilon)=1$，故在这二种情况下，

$$\mathscr{A}(d)=\{[1],\ \mathfrak{B}\},$$

其中

$$\mathfrak{B}=\begin{cases}[((-1,\ 0,\ 2p))],\ 如\ d=8p,\ 素数\ p\equiv 1(\mathrm{mod}\ 4);\\ \left[\left(\left(-1,\ 1,\ \dfrac{p_1p_2-1}{4}\right)\right)\right],\ 如\ d=p_1p_2,\end{cases}$$

在后一种情况中，素数 p_1，p_2 均 $\equiv 1(\mathrm{mod}\ 4)$，且 $p_1\neq p_2$。

在这二种情况下，有

$$d=\begin{cases}4(a^2+b^2),\ 如\ d=8p,\ 这时\ a,\ b\ 为互素的正奇数;\\ 4a^2+b^2,\quad 如\ d=p_1p_2,\ 这时\ a,\ b\ 为互素的正整数,\ b\ 奇。\end{cases}$$

相应于 d 的这一表达式，令

$$\mathfrak{A}=\begin{cases}[((a,\ 2b,\ -a))], & \text{如 } d=8p;\\ [((a,\ b,\ -a))], & \text{如 } d=p_1p_2.\end{cases}$$

容易验证

$$\mathfrak{A}^2=\left.\begin{cases}[((a^2,\ 2b,\ -1))], & \text{如 } d=8p;\\ [((a^2,\ b,\ -1))], & \text{如 } d=p_1p_2.\end{cases}\right\}\in\mathscr{A}(d).$$

于是 $\mathfrak{A}^2=\mathfrak{B}\neq[1]$，$\mathfrak{A}^4=\mathfrak{B}^2=[1]$，即 $\mathfrak{A}$ 是 $\mathscr{C}(d)$ 的一个四阶元。这证明了 $h(d)$ 是偶数。

综上所述，我们证明了下面的引理。

引理 1.34 当 d 为一个正的基本判别式时，判别式为 d 的二元二次型广义相似类群的阶 $h(d)$ 为奇数的充要条件是 $d=8$，p（素数 $p\equiv1 \pmod 4$），$4q$（素数 $q\equiv3 \pmod 4$），$8q$（素数 $q\equiv3 \pmod 4$），q_1q_2（素数 q_1，q_2 均 $\equiv3 \pmod 4$，且 $q_1\neq q_2$）。

对正的基本判别式 $d>0$，$h(d)=1$ 的情况是非常之多的。对此，Gauss 提出了下面著名的猜想。

Gauss 猜想(Ⅲ)：存在无穷多个正的基本判别式 d，使 $h(d)=1$。

另外，还有

Gauss 猜想（Ⅱ）：当负的基本判别式 $d\to-\infty$ 时，$h(d)\to+\infty$。

以上三个猜想即为著名的 Gauss 类数问题。

§2 二 次 域

2.1 二次域的理想类群

有理数域 Q 的二次扩张，称为二次数域，简称二次域。它的一般形式是 $K=Q(\sqrt{d})$，其中 d 是一个基本判别式，d 也是域 $K=Q(\sqrt{d})$ 的判别式：当 $d\equiv1 \pmod 4$ 时，它是一个无平方因子的有理整数，且 $d\neq1$；当 $d\equiv0 \pmod 4$ 时，$\frac{d}{4}$ 是一个无平方因子的有

理整数，且$\frac{d}{4}\equiv 2$或$3 \pmod 4$。今后一般地说，记号$K=Q(\sqrt{d})$中的d是K的判别式。

Galois 群$G=\mathrm{Gal}(K/Q)=\langle\sigma\rangle$是一个二阶群，$\sigma$是映射：

$$\sigma:\ K\to K,\ \sigma(a+b\sqrt{d})=a-b\sqrt{d},\ \forall a,\ b\in Q.$$

以$N(\alpha)=\alpha\sigma(\alpha)$表$\alpha\in K$的范，$T(\alpha)=\alpha+\sigma(\alpha)$表示$\alpha\in K$的迹，$\sigma(\alpha)$称为$\alpha$的共轭数，$\alpha$与$\sigma(\alpha)$是有理系数二次方程

$$x^2-T(\alpha)x+N(\alpha)=0$$

的二个根。

域$K=Q(\sqrt{d})$的整数环$O_K=Z\oplus\omega Z$（直和），其中$\omega=\frac{b_0+\sqrt{d}}{2}$，而$b_0=0$或$1$，视$d\equiv 0$或$1 \pmod 4$而定。

O_K的一个加法子群$\mathfrak{A}$称为O_K的一个整理想，简称为理想，如果它满足条件：

$$\alpha\mathfrak{A}\subseteq\mathfrak{A},\ \forall\alpha\in O_K.$$

定义O_K的两个整理想$\mathfrak{A}$与$\mathfrak{B}$的积$\mathfrak{A}\mathfrak{B}$为

$$\mathfrak{A}\mathfrak{B}=\left\{\sum_{i=1}^{n}\alpha_i\beta_i\,\middle|\,\alpha_i\in\mathfrak{A},\ \beta_i\in\mathfrak{B},\ n\in N\right\},$$

$\mathfrak{A}\mathfrak{B}$仍是O_K的整理想，易见$\mathfrak{A}\mathfrak{B}=\mathfrak{B}\mathfrak{A}$。

$\forall\alpha\in O_K$，αO_K也是O_K的一个整理想，称为主整理想，记为$[\alpha]$。特别$[0]$是O_K的一个整理想，称为零理想。O_K也是O_K的一个整理想，称为单位理想，也即$[1]$。

更一般地，对给定的$\alpha_1,\ \cdots,\ \alpha_s\in O_K$，$\alpha_1O_K+\cdots+\alpha_sO_K$也是$O_K$的一个整理想，记为$[\alpha_1,\ \cdots,\ \alpha_s]$。

对O_K的两个整理想$\mathfrak{A}$、$\mathfrak{B}$，如存在O_K的一个整理想$\mathfrak{C}$，使得

$$\mathfrak{A}=\mathfrak{B}\mathfrak{C},$$

则称$\mathfrak{B}$可除尽（或整除）$\mathfrak{A}$，记为$\mathfrak{B}\mid\mathfrak{A}$。$\mathfrak{B}$，$\mathfrak{C}$称为$\mathfrak{A}$的因子。

对O_K的两个整理想$\mathfrak{A}$，$\mathfrak{B}$，$\mathfrak{B}\mid\mathfrak{A}$的充要条件是$\mathfrak{A}\subseteq\mathfrak{B}$。

O_K的一个整理想$\mathfrak{P}$称为素理想，如果除$\mathfrak{P}$及$[1]$以外，它没有其他的因子。

对 O_K 的每一个整理想 $\mathfrak{A}$, 均存在整理想 $\mathfrak{B}$ 和一个正整数 a, 使

$$\mathfrak{A}\mathfrak{B}=[a].$$

定理 2.1 (整理想的唯一分解定理). O_K 的每一个不等于 $O_K=[1]$ 的非零整理想均可分解为有限个素理想的乘积, 而且, 如不计素因子的排列次序, 则分解方法是唯一的.

对 O_K 的两个整理想 $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{A}+\mathfrak{B}=\{\alpha+\beta \mid \alpha\in\mathfrak{A},\ \beta\in\mathfrak{B}\}$ 和 $\mathfrak{A}\cap\mathfrak{B}=\{\alpha \mid \alpha\in\mathfrak{A},\ \alpha\in\mathfrak{B}\}$ 分别称为它们的最大公因子理想和最小公倍理想, 当 $\mathfrak{A}$、$\mathfrak{B}$ 均非零时, 设它们由唯一分解定理所确定的标准分解式分别为

$$\mathfrak{A}=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_s^{e_s},\quad \mathfrak{B}=\mathfrak{P}_1^{f_1}\cdots\mathfrak{P}_s^{f_s},$$

这里 $\mathfrak{P}_1, \cdots, \mathfrak{P}_s$ 为 s 个两两不相同的素理想, $e_i, f_i (1\leqslant i\leqslant s)$ 为非负有理整数 (我们允许 e_i, f_i 中的某些为 0, 并令 $\mathfrak{P}^0=[1]=O_K$), 则 $\mathfrak{A}$ 与 $\mathfrak{B}$ 的最大公因子理想

$$\mathfrak{A}+\mathfrak{B}=\prod_{i=1}^{s}\mathfrak{P}_i^{\min(e_i,f_i)},$$

而 $\mathfrak{A}$ 与 $\mathfrak{B}$ 的最小公倍理想

$$\mathfrak{A}\cap\mathfrak{B}=\prod_{i=1}^{s}\mathfrak{P}_i^{\max(e_i,f_i)},$$

特别的, 当 $\mathfrak{A}+\mathfrak{B}=[1]=O_K$ 时, 即不存在 $[1]=O_K$ 以外的整理想是 $\mathfrak{A}$, $\mathfrak{B}$ 的公共因子理想时, $\mathfrak{A}$, $\mathfrak{B}$ 称为是互素的.

对 O_K 的任一个非零整理想 $\mathfrak{A}$, 以及 $\mathfrak{A}$ 中的每一个非零元素 α, 均存在 $\beta\in\mathfrak{A}$, 使 $\mathfrak{A}=[\alpha]+[\beta]$.

O_K 的每一个非零整理想 $\mathfrak{A}$ 可表为

$$\mathfrak{A}=am\mathbb{Z}\oplus\frac{b+\sqrt{d}}{2}m\mathbb{Z}\ (\text{直和}),$$

这里 a, b, m 为有理整数, 且满足

$$m>0;\ |b|<a \text{ 或 } b=a;\ b^2\equiv d \pmod{4a},$$

a, b, m 由 $\mathfrak{A}$ 所唯一确定, 并有

$$\mathfrak{A}=\left[am,\ \frac{b+\sqrt{d}}{2}m\right]=[m]\left[a,\ \frac{b+\sqrt{d}}{2}\right],$$

在这一表示式下,定义 $\mathfrak{A}$ 的范

$$N(\mathfrak{A})=am^2.$$

易见有 $N([\alpha])=|N(\alpha)|$, $N([0])=0$, $N([1])=1$.

如有 $\mathfrak{A}\mid[\alpha]$, 则称为 $\mathfrak{A}$ 整除 α, 记为 $\mathfrak{A}\mid\alpha$, 它等价于 $\alpha\in\mathfrak{A}$.

对 O_K 中的整数 α, β, 和 O_K 的一个非零整理想 $\mathfrak{A}$, 如有 $\mathfrak{A}\mid\alpha-\beta$, 则称 α 与 β 对模 $\mathfrak{A}$ 同余,记为

$$\alpha\equiv\beta(\bmod \mathfrak{A}).$$

以这种同余关系对 O_K 中元素进行分类,即知共有 $N(\mathfrak{A})$ 类,因此有

$$N(\mathfrak{A})=|O_K/\mathfrak{A}|.$$

对 O_K 中的两个整理想 $\mathfrak{A}$, $\mathfrak{B}$ 有

$$N(\mathfrak{A}\mathfrak{B})=N(\mathfrak{A})N(\mathfrak{B}).$$

如对 $\alpha\in O_K$, 素理想 $\mathfrak{P}$ 不整除 α, 则有

$$\alpha^{N(\mathfrak{P})-1}\equiv 1(\bmod \mathfrak{P}).$$

对 O_K 的一个整理想 $\mathfrak{A}$, $\mathfrak{A}\cap\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个理想, 这里 $\mathbb{Z}$ 是熟知的有理整数环, 所以存在一个非负有理整数 m, 使 $\mathfrak{A}\cap\mathbb{Z}=m\mathbb{Z}$, m 是 $\mathfrak{A}$ 中最小的非负有理整数, 并有 $\mathfrak{A}\mid[m]$, 即 $\mathfrak{A}\mid m$.

特别的, 对 O_K 的一个素理想 $\mathfrak{P}$, $\mathfrak{P}\cap\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个素理想, 所以存在一个有理素数 p, 使 $\mathfrak{P}\cap\mathbb{Z}=p\mathbb{Z}$, p 是 $\mathfrak{P}$ 所含的唯一的一个有理素数, 而有 $\mathfrak{P}\mid[p]$, 即 $\mathfrak{P}\mid p$.

Dedekind **判别式定理**　对任一个有理素数 p, 我们有下列素理想分解式:

$$[p]=pO_K=\begin{cases}\mathfrak{P},\ \mathfrak{P}\text{ 为一个素理想, 如 }\left(\dfrac{d}{p}\right)=-1;\\ \mathfrak{P}_1\mathfrak{P}_2,\ \mathfrak{P}_1,\ \mathfrak{P}_2\text{ 为不同的素理想, 如 }\left(\dfrac{d}{p}\right)=1;\\ \mathfrak{P}^2,\ \mathfrak{P}\text{ 为一个素理想, 如 }\left(\dfrac{d}{p}\right)=0,\end{cases}$$

这里 $\left(\dfrac{d}{p}\right)$ 为 Kronecker 符号, 在这三种情况中, p 分别称为是惯性的, 分解的, 分歧的, 并且分别有:

当$\left(\frac{d}{p}\right)=-1$时，$N(\mathfrak{P})=p^2$；

当$\left(\frac{d}{p}\right)=1$时，$\mathfrak{P}_1=[p,\ c+\sqrt{d}]$，$\mathfrak{P}_2=[p,\ a-\sqrt{d}]$，如$p$奇，其中$a$为$x^2\equiv d(\bmod\ p)$的一个解；或$\mathfrak{P}_1=\left[2,\ \frac{1+\sqrt{d}}{2}\right]$，$\mathfrak{P}_2=\left[2,\ \frac{1-\sqrt{d}}{2}\right]$，如$p=2$；并且有$N(\mathfrak{P}_1)=N(\mathfrak{P}_2)=p$；

当$\left(\frac{d}{p}\right)=0$时，$\mathfrak{P}=[p,\ \sqrt{d}]$，如$p$奇；$\mathfrak{P}=[2,\ \sqrt{d}]$，如$p=2$且$8|d$；或$\mathfrak{P}=[2,\ 1+\sqrt{d}]$，如$p=2$，$4|d$，但$8\nmid d$；并且有$N(\mathfrak{P})=p$。

域$\mathbb{K}$的一个非零子集合$\mathfrak{A}$称为$\mathbb{K}$的一个*分式理想*，如果存在$0\neq\lambda\in O_{\mathbb{K}}$，使$\lambda\mathfrak{A}$是$O_{\mathbb{K}}$的一个整理想。非零整理想当然是分式理想。对$\mathbb{K}$的每一个非零元素$\alpha$，$\alpha O_{\mathbb{K}}$也是一个分式理想，记为$[\alpha]$，称为*主分式理想*。每一个分式理想$\mathfrak{A}$均有$\mathbb{Z}$—基，即存在$\alpha_1$，$\alpha_2\in\mathfrak{A}$，使

$$\mathfrak{A}=\alpha_1\mathbb{Z}\oplus\alpha_2\mathbb{Z}\ (\text{直和})。$$

对$\mathbb{K}$的两个分式理想$\mathfrak{A}$与$\mathfrak{B}$定义$\mathfrak{A}$与$\mathfrak{B}$的乘积为

$$\mathfrak{A}\mathfrak{B}=\left\{\sum_{i=1}^{n}\alpha_i\beta_i\,|\,\alpha_i\in\mathfrak{A},\ \beta_i\in\mathfrak{B},n\in\mathbb{N}\right\},$$

$\mathfrak{A}\mathfrak{B}$也是分式理想，且$\mathfrak{A}\mathfrak{B}=\mathfrak{B}\mathfrak{A}$。由这一乘法，$\mathbb{K}$的全体分式理想组成一个自由Abel群，称为*分式理想群*，记为$I(\mathbb{K})$，且每一个分式理想$\mathfrak{A}$可以唯一地表为两个互素的非零整理想的商，也可唯一地表为下列形式：

$$\mathfrak{A}=\mathfrak{P}_1^{m_1}\cdots\mathfrak{P}_s^{m_s},$$

其中$\mathfrak{P}_1$，…，$\mathfrak{P}_s$是$O_{\mathbb{K}}$的s个互不相同的素理想，$m_i\in\mathbb{Z}-\{0\}$。对分式理想$\mathfrak{A}=\mathfrak{B}/\mathfrak{C}$，其中$\mathfrak{B}$，$\mathfrak{C}$为两个非零整理想，定义

$$N(\mathfrak{A})=N(\mathfrak{B})/N(\mathfrak{C}),$$

易见$N(\mathfrak{A})$与$\mathfrak{B}$，$\mathfrak{C}$的取法无关，并且对两个分式理想$\mathfrak{A}_1$，$\mathfrak{A}_2$，有

$$N(\mathfrak{A}_1\mathfrak{A}_2)=N(\mathfrak{A}_1)N(\mathfrak{A}_2)。$$

对主分式理想$[\alpha]$，有$N([\alpha])=|N(\alpha)|$。

$\mathbb{K}$ 的所有主分式理想在上述乘法下组成了分式理想群 $I(\mathbb{K})$ 的一个子群，记为 $P(\mathbb{K})$。

对两个分式理想 $\mathfrak{A}$, $\mathfrak{B}$，如有 $\mathfrak{A}\mathfrak{B}^{-1}\in P(\mathbb{K})$，即 $\mathfrak{A}\mathfrak{B}^{-1}$ 是一个主分式理想时，称 $\mathfrak{A}$ 与 $\mathfrak{B}$ 是相似的，记为 $\mathfrak{A}\backsim\mathfrak{B}$，这是一种等价关系，由这种等价关系给出的（分式）理想等价类是 Abel 群 $I(\mathbb{K})$相对于子群 $P(\mathbb{K})$的陪集，可以视为商群 $I(\mathbb{K})/P(\mathbb{K})$的一个元素，$P(\mathbb{K})$ 即为主(分式)理想等价类。我们把商群 $\mathscr{C}(\mathbb{K})=P(\mathbb{K})/I(\mathbb{K})$称为数域 $\mathbb{K}$ 的理想类群，简称为类群，$\mathscr{C}(\mathbb{K})$中的每一个元素称为 $\mathbb{K}$ 的一个理想类，以后把分式理想简称为理想。每一个理想类中，都存在一个代表理想

$$\left[a,\ \frac{b+\sqrt{d}}{2}\right],$$

其中 a, $b\in\mathbb{Z}$，满足 $|b|<a$ 或 $b=a$, $b^2\equiv d \pmod{4a}$，并可设 a 是属于这个理想类的最小正整数，a, b 由这个类唯一决定。由此即知$\mathscr{C}(\mathbb{K})$ 是一个有限 Abel 群，$h(d)=h(\mathbb{K})=|\mathscr{C}(\mathbb{K})|$，即 $\mathscr{C}(\mathbb{K})$的阶，称为 $\mathbb{K}$ 的理想类的类数，简称为类数。

$h(d)=1$ 等价于 $O_{\mathbb{K}}$ 是唯一因子分解的整环。

满足 α, $\alpha^{-1}\in O_{\mathbb{K}}$ 的元素 α，称为 $O_{\mathbb{K}}$ 的单位，所有的单位组成了 $O_{\mathbb{K}}$(也称为 $\mathbb{K}$)的单位群，记为 $U_{\mathbb{K}}$。它所含的单位根，即存在一个正整数 n 使 $\alpha^n=1$ 成的 α，组成了 $U_{\mathbb{K}}$ 的一个子群，称为单位根群，记为 $W_{\mathbb{K}}$。$W_{\mathbb{K}}$ 是一个有限群，以 $w_{\mathbb{K}}$ 记 $W_{\mathbb{K}}$ 的阶，即 $w_{\mathbb{K}}=|W_{\mathbb{K}}|$，我们有

$$U_{\mathbb{K}}=W_{\mathbb{K}}\otimes V_{\mathbb{K}}\ (\text{直积}),$$

其中

$$w_{\mathbb{K}}=\begin{cases}2,\\4,\\6,\end{cases}\quad W_{\mathbb{K}}=\begin{cases}\{\pm1\},\ \text{如 } d>0,\ \text{或 } d<-4;\\ \{\pm1,\ \pm\sqrt{-1}\},\ \text{如 } d=-4;\\ \left\{\pm1,\pm\left(\dfrac{-1+\sqrt{-3}}{2}\right),\pm\left(\dfrac{-1-\sqrt{-3}}{2}\right)\right\},\\ \qquad\qquad \text{如 } d=-3,\end{cases}$$

$$V_K=\begin{cases}\{1\}, & \text{如 } d<0;\\ \langle\varepsilon\rangle, & \text{如 } d>0,\end{cases}$$

这里，当 $d>0$ 时，ε 为广义 Pell 方程

$$x^2-dy^2=\pm4\quad(x,\ y\in\mathbb{Z})$$

的基本解 $\varepsilon=\frac{x_0+\sqrt{d}\,y_0}{2}$，并有 $\varepsilon>1$ 与 $N(\varepsilon)=\pm1$；ε 称为$\mathbb{K}$的基本单位；而称 Pell 方程

$$x^2-dy^2=4\quad(x,\ y\in\mathbb{Z})$$

的基本解 ε_+ 为 $\mathbb{K}$ 的全正基单位，并且有

$$\varepsilon_+=\begin{cases}\varepsilon, & \text{如 } N(\varepsilon)=1;\\ \varepsilon^2, & \text{如 } N(\varepsilon)=-1,\end{cases}$$

同时 ε_+，$\sigma(\varepsilon_+)=\varepsilon_+^{-1}$ 均大于 0(此即 ε_+ 为全正的原因，而 $\sigma(\varepsilon)=\pm\varepsilon^{-1}$ 不一定大于 0)。

以上内容及下列各小节的许多内容，请参考华罗庚著《数论导引》第十六章，以及冯克勤著《代数数论入门》(上海科学技术出版社出版)有关章节。

2.2 二次域与二次型的对应关系

二次域 $\mathbb{K}=Q(\sqrt{d})$ 的理想类与以 d 为判别式的二元二次原型的广义相似类之间有如下的对应关系：

命 $\mathfrak{A}$ 为 $\mathbb{K}$ 的一个 (分式) 理想，α_1，α_2 为 $\mathfrak{A}$ 的一组 $\mathbb{Z}$-基，即有

$$\mathfrak{A}=\alpha_1\mathbb{Z}\oplus\alpha_2\mathbb{Z}\ (\text{直和})。$$

注意对 $\mathfrak{A}$ 的一组 $\mathbb{Z}$-基 $\{\alpha_1,\ \alpha_2\}$，总有

$$(\alpha_1\sigma(\alpha_2)-\sigma(\alpha_1)\alpha_2)^2=N(\mathfrak{A})^2d,$$

故可设

$$\alpha_1\sigma(\alpha_2)-\sigma(\alpha_1)\alpha_2=N(\mathfrak{A})\sqrt{d}. \tag{2.110}$$

对应于上述的 $\mathfrak{A}$，作二次型

$$f(x,\ y)=\frac{N(\alpha_1x+\alpha_2y)}{N(\mathfrak{A})}=\frac{(\alpha_1x+\alpha_2y)(\sigma(\alpha_1)x+\sigma(\alpha_2)y)}{N(\mathfrak{A})}$$
$$=ax^2+bxy+cy^2,$$

这里

$$a=\frac{N(\alpha_1)}{N(\mathfrak{A})},\quad b=\frac{N(\alpha_1+\alpha_2)-N(\alpha_1)-N(\alpha_2)}{N(\mathfrak{A})},$$

$$c=\frac{N(\alpha_2)}{N(\mathfrak{A})}.$$

由 $\alpha_1,\ \alpha_2,\ \alpha_1+\alpha_2\in\mathfrak{A}$ 即知，$a,\ b,\ c$ 为有理整数，又 $f(x,\ y)=((a,\ b,\ c))$ 的判别式为

$$b^2-4ac=\frac{(\alpha_1\sigma(\alpha_2)-\sigma(\alpha_1)\alpha_2)^2}{N(\mathfrak{A})^2}=d,$$

这样 $f(x,\ y)$ 是一个判别式为 d 的有理整系数二元二次型，又 $d<0$ 时，$K=Q(\sqrt{d})$ 是虚域，故必有 $a>0$，从而 $f(x,\ y)$ 正定。这样定出的 $f(x,\ y)$ 称为属于 $\mathfrak{A}$ 的二次型(由于 d 为基本判别式，所以 $f(x,\ y)$ 一定是原型)。

易见，如取 $\alpha_1,\ \alpha_2$ 为 $\mathfrak{A}$ 的所有满足 (2.110) 的 $\mathbb{Z}$-基，即可得到所有与 f 相似的二次型。

反之，对于任一个以 d 为判别式的有理整系数的正定的或不定的二元二次型 $f(x,\ y)=((a,\ b,\ c))$ (因为 d 是基本判别式，f 显然是原型)，一定有 K 的一个(分式)理想 $\mathfrak{A}$ 及其一组 $\mathbb{Z}$-基，使 f 属于 $\mathfrak{A}$；先取理想

$$\mathfrak{M}=\left[a,\ \frac{-b+\sqrt{d}}{2}\right],$$

$a,\ \dfrac{b-\sqrt{d}}{2}$ 是 $\mathfrak{M}$ 的一组 $\mathbb{Z}$-基。当 $a>0$ 时，可取 $\mathfrak{A}=\mathfrak{M}$，及其一组整基；而当 $a<0$ 时，由于只考虑正定型，故必有 $d>0$，可取 $\mathfrak{A}=\sqrt{d}\,\mathfrak{M}$，及其一组整基 $a\sqrt{d},\ \dfrac{b-\sqrt{d}}{2}\sqrt{d}$。则容易验证属于 $\mathfrak{A}$ 的二次型即为 $f(x,\ y)$。

定义 2.1　如对二个(分式)理想 $\mathfrak{A}\mathfrak{B}$，存在一个 $\gamma\in K$，使

$$\mathfrak{B}=[\gamma]\mathfrak{A},\ 且\ N(\gamma)>0,$$

则称 $\mathfrak{A}$ 与 $\mathfrak{B}$ 为狭义相似的，记为 $\mathfrak{A}\approx\mathfrak{B}$。

狭义相似也是一种等价关系，狭义相似是相似的一个特殊情形，我们把原先的相似也称为广义相似。对虚域而言，广义相似即

为狭义相似。

引理 2.1 相似的二次型属于狭义相似的理想，其逆也真。

证明 见华罗庚著《数论导引》p.492。

引理 2.2 广义相似的二次型属于相似的理想，其逆也真。

证明 设α_1, α_2与β_1, β_2分别为（分式）理想$\mathfrak{A}$与$\mathfrak{B}$的$\mathbb{Z}$-基，且均满足(2.110)。令

$$f(x,\ y)=\frac{N(\alpha_1 x+\alpha_2 y)}{N(\mathfrak{A})},\ g(x,\ y)=\frac{N(\beta_1 x+\beta_2 y)}{N(\mathfrak{B})}.$$

先设$f\backsim g$，即f与g广义相似。如f与g为狭义相似的，则由引理 2.1（注意对二次型而言狭义相似与相似是一回事，而对二次域的分式理想而言广义相似与相似是一回事）即知，$\mathfrak{A}$与$\mathfrak{B}$狭义相似，因此$\mathfrak{A}$与$\mathfrak{B}$也相似。如f与g不是狭义相似的，则由定义可知必有$d>0$，且f狭义相似于$-g^{-1}$（当$g=((a,\ b,\ c))$时，$-g^{-1}\approx((-a,\ b,\ -c))$），从而有

$$\frac{N(\alpha_1 x+\alpha_2 y)}{N(\mathfrak{A})}\approx-\frac{N(\beta_1 x-\beta_2 y)}{N(\mathfrak{B})},$$

这样由定义可知，存在有理整数$r,\ s,\ t,\ u$，使$ru-st=1$，及

$$\frac{N((r\alpha_1+t\alpha_2)x+(s\alpha_1+u\alpha_2)y)}{N(\mathfrak{A})}=-\frac{N(\beta_1 x-\beta_2 y)}{N(\mathfrak{B})}. \tag{2.111}$$

由于$\dfrac{\beta_2}{\beta_1},\ \dfrac{\sigma(\beta_2)}{\beta_1}$为方程$N(\beta_1 x-\beta_2)=0$的两个根，又$-\dfrac{s\alpha_1+u\alpha_2}{r\alpha_1+t\alpha_2}$也是这个方程的根，故有

$$\frac{s\alpha_1+u\alpha_2}{r\alpha_1+t\alpha_2}=-\frac{\beta_2}{\beta_1}\ \text{或}\ -\frac{\sigma(\beta_2)}{\sigma(\beta_1)}.$$

这样，存在$\lambda\in\mathbb{K}$，使

$$r\alpha_1+t\alpha_2=\lambda\beta_1,\ s\alpha_1+u\alpha_2=-\lambda\beta_2;$$

或

$$r\alpha_1+t\alpha_2=\lambda\sigma(\beta_1),\ s\alpha_1+u\alpha_2=-\lambda\sigma(\beta_2). \tag{2.112}$$

代入(2.111)，即有

$$N(\lambda)=\lambda\sigma(\lambda)=-\frac{N(\mathfrak{A})}{N(\mathfrak{B})}<0. \tag{2.113}$$

我们来证明，只可能(2.112)成立。如若不然，则有

$$ru-st)(\alpha_1\sigma(\alpha_2)-\alpha_2\sigma(\alpha_1))=\lambda\sigma(\lambda)(\beta_1\sigma(\beta_2)-\beta_2\sigma(\beta_1)),$$

从而由 (2.110)，即有

$$N(\mathfrak{A})\sqrt{d}=N(\lambda)N(\mathfrak{B})\sqrt{d},$$

即

$$N(\lambda)=\frac{N(\mathfrak{A})}{N(\mathfrak{B})}>0.$$

这与(2.113)矛盾。

这样由 $ru-st=1$ 及(2.112)即知 $\lambda\beta_1$, $\lambda\beta_2$ 既为 $\mathfrak{A}$ 的一组 $\mathbb{Z}$-基，也是$[\lambda]\mathfrak{B}$ 的一组 $\mathbb{Z}$-基，所以有

$$\mathfrak{A}=[\lambda]\mathfrak{B},$$

即得 $\mathfrak{A}\sim\mathfrak{B}$。

反之，设 $\mathfrak{A}$ 与 $\mathfrak{B}$ 为相似的，如 $\mathfrak{A}$ 与 $\mathfrak{B}$ 为狭义相似的，则由引理 2.1 即知 f 与 g 为狭义相似，当然也广义相似。若 $\mathfrak{A}$ 与 $\mathfrak{B}$ 不是狭义相似的，则 $\mathbb{K}$ 为实域，即 $d>0$，且有

$$\mathfrak{A}=[\lambda]\mathfrak{B},\ \lambda\in\mathbb{K},\ N(\lambda)<0. \tag{2.114}$$

命 α_1, α_2 与 β_1, β_2 分别为 $\mathfrak{A}$ 与 $\mathfrak{B}$ 的 $\mathbb{Z}$-基，并均满足(2.110)，则 α_1, α_2 与 $\lambda\beta_1$, $-\lambda\beta_2$ 均为 $\mathfrak{A}$ 的$\mathbb{Z}$-基，所以存在有理整数 r, s, t, u 使

$$ru-st=\pm1,\ \lambda\beta_1=r\alpha_1+t\alpha_2,\ -\lambda\beta_2=s\alpha_1+u\alpha_2. \tag{2.115}$$

于是

$$N(\lambda)(\beta_1\sigma(\beta_2)-\beta_2\sigma(\beta_1))=-(ru-st)(\alpha_1\sigma(\alpha_2)-\alpha_2\sigma(\alpha_1)). \tag{2.116}$$

这样由(2.110)、(2.114)、(2.115)与 (2.116)，即知有

$$ru-st=1,\ \ N(\lambda)=-\frac{N(\mathfrak{A})}{N(\mathfrak{B})}. \tag{2.117}$$

由(2.115)与(2.117)知(2.111)成立，再结合(2.117)，即得

$$f\approx -g^{-1}.$$

于是 f 与 g 广义相似。引理证毕。

令 $H(d)$ 为狭义相似下的理想类的类数。$h(d)$ 为理想类的类数，则由上述引理 2.1 可知，$H(d)$是判别式为 d 的二元二次原型

类群的阶。而由引理 2.2 知，$h(d)$ 是判别式为 d 的二元二次原型广义相似类群的阶。

附注 由以上的说明，可知二元二次型广义相似类与理想类之间的对应关系是

$$[[((a,\ -b,\ -c))]] \longleftrightarrow \left[\left[a,\ \frac{b+\sqrt{d}}{2}\right]\right],$$

这里左边是二元二次型的广义相似类，右边是理想类，并可取有理整数 a, b, c 满足

$$|b| \leqslant a \leqslant |c|,\ b^2+4ac=d,$$

且 a 是属于右边理想类的最小正整数(用型的语言来叙述，则是左边(广义)类所能表出的最小正整数)，c 与 d 同号，即 $cd>0$。

由于二元二次型与理想之间的这种对应关系，我们在研究二次域的有关问题时，可以使用两种不同的语言，有时用型，有时用理想，就看哪一个便利了。

2.3 二次域的类数公式

由上一小节的引理 2.1 与引理 2.2，我们有下面的定理。

定理 2.2 设 d 为基本判别式，$h(d)$, $H(d)$ 定义见§2.2，则有

(1) $h(d)=\begin{cases} H(d), & \text{如 } d<0\text{；或 } d>0,\ \text{而 } N(\varepsilon)=-1; \\ \dfrac{H(d)}{2}, & \text{如 } d>0,\ \text{而 } N(\varepsilon)=+1, \end{cases}$

其中当 $d>0$ 时，ε 为 $Q(\sqrt{d})$ 的基本单位，以下相同。

(2) 当 $d<0$ 时，

$$h(d)=\left|\left\{(a,\ b,\ c)\in Z^3 \,\middle|\, \begin{array}{l} b^2-4ac=d, \\ -a<b\leqslant a<c, \\ \text{或 } 0\leqslant b\leqslant a=c \end{array}\right\}\right|,$$

(3) 当 $d>0$ 时，

$$h(d)=\frac{1}{2\log\varepsilon}\sum_{\substack{1\leqslant b<\sqrt{d} \\ b\equiv d \pmod 2}}\left(\sum_{\substack{\frac{\sqrt{d}-b}{2}<a<\frac{\sqrt{d}+b}{2} \\ a \mid \frac{d-b^2}{4}}} 1\right)\log\frac{\sqrt{d}+b}{\sqrt{d}-b},$$

(4) $$h(d)=\begin{cases}\dfrac{\sqrt{d}\,L(1,\ \chi_d)}{2\log\varepsilon}, & \text{如 } d>0;\\[2ex] \dfrac{w\sqrt{d}\,L(1,\ \chi_d)}{2\pi}, & \text{如 } d<0,\end{cases}$$

其中 $\chi_d(*)=\left(\frac{d}{*}\right)$为 Kronecker 符号，$w$ 是$Q(\sqrt{d})$ 的单位根群的阶，即

$$w=\begin{cases}2, & \text{如 } d<-4;\\ 4, & \text{如 } d=-4;\\ 6, & \text{如 } d=-3,\end{cases}$$

以及

$$L(1,\ \chi_d)=\sum^{\infty}\frac{\chi_d(n)}{n},$$

(5) $$h(d)=\frac{w}{2\left(2-\left(\frac{d}{2}\right)\right)}\sum_{1<s<\frac{|d|}{2}}\left(\frac{d}{s}\right),\ \text{如 } d<0;$$

$$h(d)=-\frac{1}{\log\varepsilon}\sum_{1<s<\frac{d-1}{2}}\left(\frac{d}{s}\right)\log\sin\frac{s\pi}{d},\ \text{如 } d>0.$$

我们指出这里 log 是自然对数。

证明 (1)—(4) 由本章 §1 的二元二次型广义相似类数的公式可得。(5)见华罗庚著《数论导引》p.496 的定理 16.13.3.。

2.4 二次域的 genus 理论

本节只考虑狭义理想类群$\mathscr{C}_0(d)$。由二次型与理想的对应关系，我们有

$$\mathscr{A}(d)\approx\mathscr{C}_0(d)/\mathscr{C}_0(d)^2,$$

这里

$$\mathscr{A}(d)=\{\mathfrak{A}\in\mathscr{C}_0(d)\mid\mathfrak{A}^2=[[1]]\},$$

$$\mathscr{C}_0(d)^2=\{\mathfrak{A}\in\mathscr{C}_0(d)\mid\exists\mathfrak{B}\in\mathscr{C}_0(d),\ \text{使 } \mathfrak{A}=\mathfrak{B}^2\},$$

其中$[[1]]=[O_K]$；$\mathscr{A}(d)$称为 Ambiguous 类群，$\mathscr{C}_0(d)/\mathscr{C}_0(d)^2$称为族群，它们是同构的，它们的共同阶

$$g(d)=|\mathscr{A}(d)|=|\mathscr{C}_0(d)/\mathscr{C}_0(d)^2|=2^{\lambda-1},$$

这里 λ 是 d 所含的素因子的个数。

$\mathscr{C}_0(d)/\mathscr{C}_0(d)^2$ 的每一个元素称为一个族；单位理想所在的类，即 $[[1]]=[O_K]$ 称为主类；主类所在的族，称为主族，主族中的类均为平方类；每族所含的类数相同。由定义有

$$H(d)=g(d)\cdot|\mathscr{C}_0(d)^2|, \tag{2.118}$$

所以有

$$2^{\lambda-1}\mid H(d), \tag{2.119}$$

λ 是 d 所含素因子的个数。

$\mathscr{A}(d)$ 与 $\mathscr{C}_0(d)/\mathscr{C}_0(d)^2$ 作为 Abel 群，它们的特征群同构，并同构于自身。每一个这样的特征，我们称为 $\mathscr{C}_0(d)$ 的一个 genus 特征。由二元二次型的 genus 特征理论可知，每一个这样的特征 χ 都相应于 d 的一个如下的分解

$$d=d_1d_2,$$

其中 d_1，d_2 仍为基本判别式或 1，且对每一个理想 $\mathfrak{A}$，

$$\chi(\mathfrak{A})=\left(\frac{d_1}{N(\alpha)/N(\mathfrak{A})}\right),$$

这里 $\left(\frac{d_1}{*}\right)$ 是 Kronecker 符号，$\alpha\in\mathfrak{A}$，使 $g.c.d.(N(\alpha)/N(\mathfrak{A}),d)=1$。

显然，对于属于同一个族的理想 $\mathfrak{A}$ 与 $\mathfrak{B}$，有 $\chi(\mathfrak{A})=\chi(\mathfrak{B})$。

反之，相应于 d 的上述分解而定义的 χ，也是 $\mathscr{C}_0(d)$ 的一个 genus 特征。

特别取 d_1 为除尽 d 的素判别式（所谓素判别式是仅含一个素因子的基本判别式）时，我们得到 $\mathscr{C}_0(d)$ 的 λ 个 genus 特征，其中的任意 $\lambda-1$ 个都是独立的，并生成 $\mathscr{C}_0(d)$ 的所有 $2^{\lambda-1}$ 个 genus 特征。一般我们称这 λ 个 genus 特征在每个族的取值 (±1) 所组成的 λ 数组为该族的特征系。两个族相同的充要条件是它们的特征系相同。特别，主族的特征系是 $(\underbrace{1,\cdots,1}_{\lambda\text{个}})$。

2.5 二次域的 Gauss 类数猜想

把§1.9中关于二元二次型的Gauss猜想翻译为二次域的语言，则是：

Gauss **猜想 I**：只存在九个类数 $h(d)=1$ 的虚二次域，即

$d=-3,\ -4,\ -7,\ -8,\ -11,\ -19,\ -43,\ -67,\ -163$

的二次域 $Q(\sqrt{d})$。

Gauss **猜想 II**：$h(d)\to+\infty$，如 $d\to-\infty$。

Gauss **猜想 III**：存在无穷多个类数 $h(d)=1$ 的实二次域 $Q(\sqrt{d})$。

由§1.9的结果，我们有下面的引理。

引理 2.3 $h(d)$ 为奇数的二次域是且仅是其判别式

$$d=-4,\ \pm8,\ -q,\ p,\ 4q,\ 8q,\ q_1q_2,$$

的二次域 $Q(\sqrt{d})$，其中 $p\equiv1\pmod 4$，p 是素数，q_1，q_2，$q\equiv3\pmod 4$，也都是素数，且 $q_1\neq q_2$。

所以 $h(d)=1$ 的二次域 $Q(\sqrt{d})$ 只能在上述类型的域中找到。

由解析类数公式可以看到，$L(1,\ \chi_d)$ 与基本单位 ε 起着非常重要的基本作用。所以需进一步研究 $L(1,\ \chi)$ 与 ε，后者我们已在第一章中做过一些了，由此得出实二次域的许多结论。而 $L(1,\ \chi_d)$ 正是 Dirichlet 级数

$$L(s,\ \chi_d)=\sum_{n=1}^{\infty}\frac{\chi_d(n)}{n^s},\ \mathrm{Re}s>1$$

在 $s=1$ 处的值，这将在第三章中讨论。

本 章 评 注

1. 本章的许多内容是经典的，可参考参考文献 [6]、[16]、[18]、[19]和[35]。

2. 二元二次型的广义相似似乎是本书首次引入的。这样，处

理起二次域与二次型的对应关系,可以方便些。

3. 定理 1.3 采自参考文献 [52], 引理 1.27 与引理 1.28 采自参考文献[60]。

4. 定理 1.4 给出二元二次型合成的一个较为简便的算法。

5. 定理 1.8 以及引理 1.29、1.30 与 1.31 为本书首次发表的。

6. 本章给出了二元二次型与二次域经典理论一个相当系统的阐述,特别对 genus 特征给出了较为明确的阐述,对以后的研究,自然是有帮助的。

第 3 章

Dedekind ζ-函数与极限公式

本章的内容是讨论二次域的 Dedekind ζ- 函数以及相关的 L 函数，并求出它们在 $s=1$ 处的极限公式，特别关于虚二次域方面的结果是经典的。实二次域方面的结果需要对所谓的 Dedekind η-函数的变换公式作一些研究。本章的内容为以后几章作了很好的准备。

§1　二次域的 Dedekind ζ-函数

1.1　Dedekind ζ-函数

设 $K=Q(\sqrt{d})$ 是一个判别式为 d 的二次域，$\mathscr{C}(d)$ 为 K 的（广义）理想类群，$\mathscr{C}_0(d)$ 为 K 的狭义理想类群。对每一个 $A\in\mathscr{C}(d)$，令

$$\zeta_K(s\,|\,A)=\sum_{\mathfrak{A}\in A}\frac{1}{N(\mathfrak{A})^s},\ \operatorname{Re}s>1, \tag{3.1}$$

其中 $\mathfrak{A}$ 跑过 A 中的所有非零整理想，$\zeta_K(s\,|\,A)$ 称为理想类 A 的 ζ-函数。它有以下性质：

(1) $\zeta_K(s\,|\,A)$ 可以开拓为 s 的一个半纯函数，它仅在 $s=1$ 处有一个孤立奇点，且为单极点，其残数为

$$\rho_K=\begin{cases}\dfrac{2\log\varepsilon}{\sqrt{d}}, & \text{如 } d>0;\\[2ex] \dfrac{2\pi}{w\sqrt{|d|}}, & \text{如 } d<0,\end{cases} \tag{3.2}$$

其中 ε 是基本单位，w 是单位根群的阶，注意 ρ_K 与 A 无关；

(2) $\zeta_K(s\,|\,A)$ 满足下列函数方程：

$$F_{\mathbb{K}}(s\mid A)\overset{\text{def}}{=\!=}\left(\frac{\sqrt{|d|}}{2^r\pi}\right)^s\Gamma\left(\frac{s}{2}\right)^{2(1-r)}\Gamma(s)^r\zeta_{\mathbb{K}}(s\mid A)$$
$$=F_{\mathbb{K}}(1-s\mid A),\tag{3.3}$$

这里$\Gamma(*)$是Γ函数,而

$$r=\begin{cases}0, & \text{如 } d>0;\\ 1, & \text{如 } d<0.\end{cases}$$

命

$$\zeta_{\mathbb{K}}(s)=\sum_{A\in\mathscr{C}(d)}\zeta_{\mathbb{K}}(s\mid A)=\sum_{\mathfrak{A}}\frac{1}{N(\mathfrak{A})^s},\ \operatorname{Re}s>1,\tag{3.4}$$

这里A跑过$\mathscr{C}(d)$中所有的理想类,$\mathfrak{A}$跑过$\mathbb{K}$的所有非零整理想。$\zeta_{\mathbb{K}}(s)$称为二次域$\mathbb{K}=Q(\sqrt{d})$的Dedekind ζ-函数,它有下列性质:

(1) $\zeta_{\mathbb{K}}(s)$是s的一个半纯函数,它仅在$s=1$处有一个孤立奇点,且为单极点,其线数为$h_{\mathbb{K}}\rho_{\mathbb{K}}$,其中$h_{\mathbb{K}}$为$\mathbb{K}=Q(\sqrt{d})$的类数,即$h_{\mathbb{K}}=|\mathscr{C}(d)|$,$\rho_{\mathbb{K}}$定义如(3.2);

(2) $\zeta_{\mathbb{K}}(s)$满足函数方程:

$$F_{\mathbb{K}}(s)\overset{\text{def}}{=\!=}\left(\frac{\sqrt{|d|}}{2^r\pi}\right)^s\Gamma\left(\frac{s}{2}\right)^{2(1-r)}\Gamma(s)^r\zeta_{\mathbb{K}}(s)=F_{\mathbb{K}}(1-s)\tag{3.5}$$

其中$r=0$或1,视$d>0$或$d<0$而定;

(3) 我们有Euler乘积:

$$\zeta_{\mathbb{K}}(s)=\prod_{\mathfrak{P}}\frac{1}{1-N(\mathfrak{P})^{-s}},\ \operatorname{Re}s>1,\tag{3.6}$$

这里$\mathfrak{P}$跑过$\mathbb{K}$的所有(真)素理想;

(4) $\zeta_{\mathbb{K}}(s)=\zeta(s)L(s,\chi_d)$, (3.7)

其中$\zeta(s)$为通常的Riemann ζ-函数,$L(s,\chi_d)$是Dirichlet L-函数:

$$L(s,\chi_d)=\sum^{\infty}\frac{\chi_d(n)}{n^s},\ \operatorname{Re}s>0,\tag{3.8}$$

而$\chi_d(*)=\left(\frac{d}{*}\right)$是Kronecker符号。

更一般些,对$\mathscr{C}(d)$的任一个特征χ,可以定义L-级数(或称

L-函数)

$$L(s, \chi)=\sum_{\mathfrak{A}}\chi(\mathfrak{A})N(\mathfrak{A})^{-s},\ \operatorname{Re}s>1, \tag{3.9}$$

这里 $\mathfrak{A}$ 跑过 $\mathbb{K}$ 的所有非零整理想。

考虑到 $\zeta_{\mathbb{K}}(s|A)$ 的上述性质，我们可得在$s=1$附近的 Laurent 展开式

$$\zeta_{\mathbb{K}}(s|A)=\frac{\rho_{\mathbb{K}}}{s-1}+\xi_0(A)+\xi_1(A)(s-1)+\cdots \tag{3.10}$$

这里 $\xi_0(A)$, $\xi_1(A)$, …等等是仅与A有关的常数。

于是由(3.1)、(3.9), (3.10)即有

$$\begin{aligned}L(s, \chi)&=\sum_{A\in\mathscr{F}(d)}\chi(A)\zeta_{\mathbb{K}}(s|A)\\&=\frac{\rho_{\mathbb{K}}}{s-1}\sum_{A\in\mathscr{F}(d)}\chi(A)+\sum_{A\in\mathscr{F}(d)}\chi(A)\xi_0(A)\\&\quad+O(|s-1|).\end{aligned} \tag{3.11}$$

这样，$L(s, \chi)$也具有相应的解析开拓和函数方程，并且当 χ 不是主特征时，$L(s, \chi)$是整函数，并有

$$L(1, \chi)=\sum_{A\in(\mathscr{F}d)}\chi(A)\xi_0(A),\ \chi\neq\chi_0. \tag{3.12}$$

$\chi=\chi_0$ 时 $L(s, \chi)=\zeta_{\mathbb{K}}(s)$。

公式

$$\lim_{s\to1}\left(\zeta_{\mathbb{K}}(s|A)-\frac{\rho_{\mathbb{K}}}{s-1}\right)=\xi_0(A)$$

称为 Kronecker 极限公式，这是因为 Kronecker 首先对虚二次域 $\mathbb{K}$ 算出了 $\xi_0(A)$的具体值。

一般说来，算出种种 ζ-函数或 L-函数在某个特定点(一般是奇点)处的 Taylor 展开式或 Laurent 展开式的常数项，即称为 Kronecker 极限公式，其推论将带来许多数论上的结论。

本小节内容，可参考 E. Hecke[28] 的书。

1.2　Dedekind η-函数及其变换公式

命H为上半平面，即

$$H=\{z\in\boldsymbol{C}\,|\,\operatorname{Im}z>0\}.$$

定义 Dedekind η-函数如下：

$$\eta(z)=q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n),\ q=e^{2\pi iz},\ z\in H. \tag{3.13}$$

因为对所有 $z\in H$，有 $\eta(z)\neq 0$，所以可以取对数，当然要取定一枝。可以定义

$$\log\eta(z)=\frac{\pi iz}{12}-\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{2\pi inz},\ z\in H, \tag{3.14}$$

这里

$$\sigma(n)=\sum_{1\leqslant m\mid n}m \tag{3.15}$$

是 n 的所有正因子的和。这等于说，我们取

$$\log(1-e^{2\pi iz})=-\sum_{n=1}^{\infty}\frac{1}{n}e^{2\pi inz},\ z\in H, \tag{3.16}$$

也即约定

$$\arg e^{i\varphi}=\varphi,\ -\pi<\varphi\leqslant\pi. \tag{3.17}$$

我们有下面的定理。

定理 1.1(Rademacher[89]) 在模变换

$$z\mapsto M\langle z\rangle=\frac{az+b}{cz+d},\quad M=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in Sl_2(\mathbb{Z})$$

下，$\log\eta(z)$ 的变换公式是

$$\log\eta(M\langle z\rangle)=\log\eta(z)+\frac{\pi i}{12}\Phi(M)$$
$$+\frac{1}{2}(\operatorname{sign}c)^2\log\frac{(\operatorname{sign}c)(cz+d)}{i}, \tag{3.18}$$

这里 sign c 是 c 的符号，即 $\operatorname{sign}c=0,\ 1,\ -1$ 视 $c=0,\ c>0,\ c<0$ 而定，

$$\Phi(M)=\begin{cases}\dfrac{b}{d}, & 如\ c=0;\\[2mm] \dfrac{a+d}{c}-12(\operatorname{sign}c)s(d,\ |c|), & 如\ c\neq 0,\end{cases} \tag{3.19}$$

其中用到所谓的 Dedekind 和

$$s(h,\ k)=\sum_{r(\bmod k)}\left(\left(\frac{r}{k}\right)\right)\left(\left(\frac{hr}{k}\right)\right),$$

$$h,\ k\in\mathbb{Z},\ k\geqslant 1,\ g.c.d.(h,\ k)=1, \tag{3.20}$$

这里用了符号

$$((x))=\begin{cases}\{x\}-\dfrac{1}{2}, & \text{如 } x \text{ 不是一个整数；}\\ 0, & \text{如 } x \text{ 是一个整数，}\end{cases}$$

而 $\{x\}$ 是 x 的小数部分。

我们有

$$\Phi(-M)=\Phi(M),\ \forall M\in SL_2(\mathbb{Z}); \tag{3.21}$$

$$\Phi(M^{-1})=-\Phi(M),\ \forall M\in SL_2(\mathbb{Z}); \tag{3.22}$$

$$\Phi(M)=\Phi(M_1)+\Phi(M_2)-3\operatorname{sign}(cc_1c_2), \tag{3.23}$$

这里 $M_1=\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}$, $M_2=\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}$, $M=\begin{pmatrix}a & b\\ c & d\end{pmatrix}=M_1M_2$,

均 $\in SL_2(\mathbb{Z})$

容易证明

$$s(h,\ k)=s(h_1,\ k),\ \text{如 } h\equiv h_1(\mathrm{mod}\,k); \tag{3.24}$$

$$s(h,\ k)=s(h',\ k),\ \text{如 } hh'\equiv 1(\mathrm{mod}\,k). \tag{3.25}$$

还有互反律：

$$12s(h,\ k)+12s(k,\ h)=-3+\frac{h}{k}+\frac{k}{h}+\frac{1}{kh},$$
$$\text{如 } h,\ k>0,\ \text{且 } g.c.d.(h,\ k)=1. \tag{3.26}$$

设 $\dfrac{h}{k}$ 的简单连分数展开式为

$$\frac{h}{k}=[a_0,\ a_1,\ \cdots,\ a_r],$$

则有：

$$\begin{aligned}s(h,\ k)=\frac{-1+(-1)^r}{8}+\frac{1}{12}\big([0,\ a_1,\ \cdots,\ a_r]\\ +(-1)^{r+1}[0,\ a_r,\ a_{r-1},\ \cdots,\ a_2,\ a_1]\\ +a_1-a_2+\cdots+(-1)^{r+1}a_r\big).\end{aligned} \tag{3.27}$$

上述的定理 1.1 以及 (3.21)—(3.26) 的证明可见所引的 Rademacher[89] 的书。(3.27) 可由 (3.26) 经归纳证明，详细见 D.J.Hickerson[32]。

对一个实二次无理数 α，设它的简单连分数展开式为：

$$\alpha=[\hat{a}_0,\ \cdots,\ \hat{a}_s,\ \overline{a_1,\ \cdots,\ a_k}],$$

这里 $\overline{a_1,\ \cdots,\ a_k}$ 是基本周期，我们称

$$\Psi(\alpha)=\begin{cases}\sum\limits_{j=1}^{k}(-1)^{j+s}a_j, & \text{如 } k \text{ 偶;}\\ 0, & \text{如 } k \text{ 奇}\end{cases} \tag{3.28}$$

为 α 的 Hirzebruch 和。

由定义，易见

$$\Psi(\alpha)=(\det M)\Psi(\beta),\ \text{如 } \alpha=M\langle\beta\rangle,\ M \text{ 为有理整系数的二阶方阵，且 } \det M=\pm1. \tag{3.29}$$

本小节的主要目的是证明下面的定理。

定理 1.2 设 $M=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})$，则有

(1) 如 $c=0$，即 M 为一个抛物元，则 $\Phi(M)=\dfrac{b}{d}$；

(2) 如 $c\neq0$，但有 $a+d=\pm2$，此时 M 仍为一个抛物元，则

$$\Phi(M)=(3-g.c.d.(b,\ c))\operatorname{sign}(c(a+d));$$

(3) 如 $c\neq0$，而 $a+d=0$ 或 ±1，此时 M 为一个椭圆元，则

$$\Phi(M)=(a+d)\operatorname{sign}c;$$

(4) 如 $c\neq0$，而 $|a+d|>2$，此时 M 为一个双曲元，则

$$\Phi(M)=\left(3+m_0\Psi\left(\frac{a-d+\sqrt{(a+d)^2-4}}{2|c|}\right)\right)\operatorname{sign}(c(a+d)),$$

这儿正整数 m_0 如下定义，令

$$u=|a+d|,\ v=g.c.d.(a-d,\ b,\ c),\ D=v^{-2}(u^2-4),$$

则 D 是一个正整数，且不是一个完全平方，那么 m_0 由下式定义：

$$\frac{u+v\sqrt{D}}{2}=\left(\frac{u_0+v_0\sqrt{D}}{2}\right)^{m_0},$$

其中 $\dfrac{u_0+v_0\sqrt{D}}{2}$ 是 Pell 方程

$$x^2-Dy^2=4$$

的基本解。

证明

(1) $c=0$ 时，由定理1.1即得。

(2) $c\neq 0$，而 $a+d=\pm 2$ 时，由(3.21)知 $\Phi(-M)=\Phi(M)$，可设 $c>0$，$a+d=\pm 2$，即应证明

$$\Phi(M)=(3-g.c.d.(b,\ c))\operatorname{sign}(a+d),\ \text{如}\ c>0\ \text{且}\ a+d=\pm 2. \tag{3.30}$$

命 $r=g.c.d.(b,\ c)$，则由

$$1=ad-bc=a(\pm 2-a)-bc,\quad (a\mp 1)^2=-bc,$$

可得

$$c=c_1^2r,\ b=-b_1^2r,\ b_1,\ c_1\in\mathbb{Z},\ g.c.d.(b_1,\ c_1)=1.$$

适当地选取 b_1，c_1 的符号，即有

$$a=b_1c_1r\pm 1,\ d=-b_1c_1r\pm 1.$$

取 $a_1, d_1\in\mathbb{Z}$，使

$$a_1c_1+b_1d_1=1.$$

则有

$$\begin{aligned}M=\begin{pmatrix}a & b\\ c & d\end{pmatrix}&=\begin{pmatrix}b_1c_1r\pm 1 & -b_1^2r\\ c_1^2r & -b_1c_1r\pm 1\end{pmatrix}\\&=\begin{pmatrix}\pm a_1+b_1r & \pm b_1\\ \mp d_1+c_1r & \pm c_1\end{pmatrix}\begin{pmatrix}c_1 & -b_1\\ d_1 & a_1\end{pmatrix}\\&=\begin{pmatrix}a_1 & b_1\\ -d_1 & c_1\end{pmatrix}\begin{pmatrix}\pm 1 & 0\\ r & \pm 1\end{pmatrix}\begin{pmatrix}a_1 & b_1\\ -d_1 & c_1\end{pmatrix}^{-1}.\end{aligned} \tag{3.31}$$

由(3.22)、(3.23)和(3.31)可得

$$\begin{aligned}\Phi(M)&=\Phi\left(\begin{pmatrix}\pm 1 & 0\\ r & \pm 1\end{pmatrix}\right)=\Phi\left(\begin{pmatrix}1 & 0\\ \pm r & 1\end{pmatrix}\right)\\&=\pm\Phi\left(\begin{pmatrix}1 & 0\\ r & 1\end{pmatrix}\right)=\pm\left(\frac{2}{r}-12s(1,\ r)\right)\end{aligned} \tag{3.32}$$

又易知有

$$s(1,\ r)=\frac{(r-1)(r-2)}{12r}. \tag{3.33}$$

由(3.32)与(3.33)即有

$$\Phi(M)=\pm(3-r),$$

此即(3.30)。证明了所需。

(3) 设 $a+d=0$ 或 ±1，于是 $c\neq0$。这时

$$z_0=\frac{a-d+(\operatorname{sign}c)\sqrt{(a+d)^2-4}}{2c}\in H$$

是M的一个不动点。易见

$$cz_0+d=\begin{cases}(\operatorname{sign} c)i, & \text{如 } a+d=0;\\ \dfrac{1}{2}+(\operatorname{sign}c)\dfrac{\sqrt{3}}{2}i, & \text{如 } a+d=1;\\ -\dfrac{1}{2}+(\operatorname{sign}c)\dfrac{\sqrt{3}}{2}i, & \text{如 } a+d=-1.\end{cases}$$

由此及变换公式(定理 1.1)即有

$$\begin{aligned}\Phi(M)&=-\frac{1}{\pi}\operatorname{Im}\log\frac{(cz_0+d)\operatorname{sign}c}{i}\\&=-\frac{1}{\pi}\arg\frac{(cz_0+d)\operatorname{sign}c}{i}=(a+d)\operatorname{sign}c,\end{aligned}$$

得到所需。

(4) 最后，如M为一个双曲元，即 $c\neq0$ 并有 $|a+d|>2$ 时。

由 $\Phi(-M)=\Phi(M)$，可设 $c>0$(M变为$-M$之后，m_0显然没变，$\operatorname{sign}(c(a+d))$也没变，还应证明

$$\Psi\left(\frac{d-a+\sqrt{(a+d)^2-4}}{2|c|}\right)=\Psi\left(\frac{a-d+\sqrt{(a+d)^2-4}}{2|c|}\right),$$

这一点在最后证明)。

令

$$|a+d|=u,\ g.c.d.(a-d,\ b,\ c)=v,\ a-d=vB,$$
$$b=-vC,\ c=vA. \tag{3.34}$$

则 $u,\ v,\ A,\ B,\ C\in\mathbb{Z}$，且有

$$u>2,\ v>0,\ A>0,\ g.c.d.(A,\ B,\ C)=1. \tag{3.35}$$

再设

$$D=B^2-4AC. \tag{3.36}$$

由(3.34)与(3.36)有

$$v^2D=v^2B^2-4AvCv=(a-d)^2+4bc=(a+d)^2-4,$$

即有

$$u^2-v^2D=4. \tag{3.37}$$

由此即知 D 是一个正整数，且 D 不是完全平方。又由(3.34)有

$$a=\frac{\pm u+vB}{2},\quad d=\frac{\pm u-vB}{2}. \tag{3.38}$$

因此有

$$M=\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} \frac{\pm u+vB}{2} & -Cv \\ Av & \frac{\pm u-vB}{2} \end{pmatrix}. \tag{3.39}$$

容易证明Dedekind 和有性质

$$s(-h,\ k)=-s(h,\ k),$$

由此，(3.39)及定理1.1. 即有

$$\begin{aligned} \Phi(M)&=\pm\left(\frac{u}{Av}-12s\left(\frac{u\mp vB}{2},\ Av\right)\right) \\ &=\pm\left(\frac{u}{Av}-12s\left(\frac{u+v|B|}{2},\ Av\right)\right). \end{aligned} \tag{3.40}$$

最后一步还用了(3.25)。

由二元二次型的约化理论(第二章§1.1)可知，存在 $r,\ r_1,\ s,\ t\in\mathbb{Z}$，使有：

$$rr_1-st=1, \tag{3.41}$$

$$\delta\tilde{A}=Ar_1^2+Br_1t+Ct^2, \tag{3.42}$$

$$\delta\tilde{B}=2Ar_1s+B(r_1r+st)+2Ctr, \tag{3.43}$$

$$\delta\tilde{C}=As^2+Bsr+Cr^2, \tag{3.44}$$

其中 $\tilde{A},\ \tilde{B},\ \tilde{C}\in\mathbb{Z}$，且有

$$|\tilde{B}|\leqslant\tilde{A}\leqslant-\tilde{C},\ \delta=\pm1. \tag{3.45}$$

$$D=\tilde{B}^2-4\tilde{A}\tilde{C},\ g.c.d.(\tilde{A},\ \tilde{B},\ \tilde{C})=1. \tag{3.46}$$

令

$$\begin{aligned} \tilde{M}=\begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix}&=\begin{pmatrix} r & s \\ t & r_1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} r & s \\ t & r_1 \end{pmatrix}^{-1} \\ &=\begin{pmatrix} ar+cs & br+ds \\ at+cr_1 & bt+dr_1 \end{pmatrix}\begin{pmatrix} r_1 & -s \\ -t & r \end{pmatrix} \end{aligned} \tag{3.47}$$

则 $\widetilde{M}\in Sl_2(\mathbb{Z})$。再命

$$\tilde{u}=|\tilde{a}+\tilde{d}|,\ \tilde{v}=g.c.d.(\tilde{a}-\tilde{d},\ \tilde{b},\ \tilde{c}),\tag{3.48}$$

则有

$$\tilde{u}=|\tilde{a}+\tilde{d}|=|a+d|=u,\tag{3.49}$$

由(3.47)有

$$\tilde{a}=arr_1-brt+csr_1-dst,\tag{3.50}$$

$$\tilde{b}=-ars+br^2-cs^2+dsr,\tag{3.51}$$

$$\tilde{c}=atr_1-bt^2+cr_1^2-dr_1t,\tag{3.52}$$

$$\tilde{d}=-ats+btr-cr_1s+dr_1r.\tag{3.53}$$

由(3.34)及(3.50)—(3.53)有

$$\begin{aligned}\tilde{a}-\tilde{d}&=(a-d)(r_1r+st)-2brt+2cr_1s\\&=vB(r_1r+st)+2Cvrt+2Avr_1s=v\delta\widetilde{B}.\end{aligned}$$

最后一步用了(3.43)，即有

$$\tilde{a}-\tilde{d}=v\delta\widetilde{B},\tag{3.54}$$

同样可得

$$\tilde{b}=-v\delta\widetilde{C},\ \tilde{c}=v\delta\widetilde{A}.\tag{3.55}$$

于是由(3.46)、(3.54)和(3.55)有

$$\tilde{v}=g.c.d.(\tilde{a}-\tilde{d},\ \tilde{b},\ \tilde{c})=vg.c.d.(\widetilde{A},\ \widetilde{B},\ \widetilde{C})=v,$$

即有

$$\tilde{v}=v.\tag{3.56}$$

(3.49)—(3.56)推出

$$\widetilde{M}=\begin{pmatrix}\tilde{a}&\tilde{b}\\\tilde{c}&\tilde{d}\end{pmatrix}=\delta\begin{pmatrix}\dfrac{\pm u\delta+v\widetilde{B}}{2}&-\widetilde{C}v\\\widetilde{A}v&\dfrac{\pm u\delta-v\widetilde{B}}{2}\end{pmatrix}.\tag{3.57}$$

当 $\delta=1$ 时，有 $\tilde{c}>0$(注意(3.55))，故由 (3.47)和(3.23)有

$$\Phi(M)=\Phi(\widetilde{M}),\ 如\ \delta=1.\tag{3.58}$$

当 $\delta=-1$ 时，由(3.55)，$\tilde{b}=\widetilde{C}v<0$，故由

$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}\tilde{a}&\tilde{b}\\\tilde{c}&\tilde{d}\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}\tilde{d}&-\tilde{c}\\-\tilde{b}&\tilde{a}\end{pmatrix},$$

即得

$$\Phi(M)=\Phi\left(\begin{pmatrix}\tilde{d} & -\tilde{c}\\ -\tilde{b} & \tilde{a}\end{pmatrix}\right), \text{ 如 } \delta=-1. \tag{3.59}$$

令

$$\omega=\frac{|\tilde{B}|+\sqrt{D}}{2\tilde{A}}. \tag{3.60}$$

由第 1 章即知 ω 的简单连分数展开式如下形状：

$$\omega=[a_0, \overline{a_1, \cdots, a_k}], \tag{3.61}$$

其中 $\overline{a_1, \cdots, a_k}$ 为基本周期，且有

$$a_k=2a_0 \text{ 或 } 2a_0-1 \tag{3.62}$$

ω 的第 l 个完全商

$$[a_l, a_{l+1}, \cdots]=\frac{P_l+\sqrt{D}}{2Q_l}(l\geqslant 0), \tag{3.63}$$

满足(P_l, $Q_l\in\mathbb{Z}$)

$$Q_0=\tilde{A},\ P_0=|\tilde{B}|,\ P_1=2a_0\tilde{A}-|\tilde{B}|; \tag{3.64}$$

$$Q_l=(-1)^l(\tilde{A}p_{l-1}^2-|\tilde{B}|p_{l-1}q_{l-1}+\tilde{C}q_{l-1}^2),\ (l\geqslant 1); \tag{3.65}$$

$$P_l=(-1)^{l-1}(2\tilde{A}p_{l-1}p_{l-2}-|\tilde{B}|(p_{l-1}q_{l-2}+p_{l-2}q_{l-1})+2\tilde{C}q_{l-1}q_{l-2}),\ (l\geqslant 2). \tag{3.66}$$

其中 $\frac{p_l}{q_l}$ 是 ω 的第 l 个渐近分数，并有

$$p_lq_{l-1}-p_{l-1}q_l=(-1)^{l-1},\ (l\geqslant 1); \tag{3.67}$$

$$P_l^2+4Q_lQ_{l-1}=D,\ (l\geqslant 1); \tag{3.68}$$

$$P_{l+1}+P_l=2a_lQ_l,\ (l\geqslant 0); \tag{3.69}$$

$$Q_l\geqslant 1(l\geqslant 0),\ P_l\geqslant 1(l\geqslant 1); \tag{3.70}$$

$$a_l=\left[\frac{P_l+\sqrt{D}}{2Q_l}\right](l\geqslant 0); \tag{3.71}$$

$$Q_k=Q_0=\tilde{A},\ P_k=2(a_k-a_0)\tilde{A}+|\tilde{B}|. \tag{3.72}$$

令

$$p=\frac{u+v|\tilde{B}|}{2},\ q=v\tilde{A}. \tag{3.73}$$

由(3.57)，即有 $g.c.d.(p, q)=1$。再由(3.46)、(3.37)、(3.73)

和(3.45),

即有

$$\widetilde{A}p^2-|\widetilde{B}|pq+\widetilde{C}q^2=\widetilde{A}<\frac{\sqrt{D}}{2},$$

因此由第一章的引理 1.7，即知 $\frac{p}{q}$ 是 ω 的一个渐近分数，即存在正整数 $l\geqslant 1$，使

$$p=p_{l-1},\ q=q_{l-1}.$$

所以由(3.65)有

$$Q_l=\widetilde{A},\ \text{且 } l \text{ 偶},\ l\geqslant 2. \tag{3.74}$$

所以(3.73)即为

$$p_{l-1}=\frac{u+v|\widetilde{B}|}{2},\ q_{l-1}=v\widetilde{A}. \tag{3.75}$$

由(3.67)及

$$p_{l-1}\frac{u-v|\widetilde{B}|}{2}+q_{l-1}\widetilde{C}v=\frac{u^2-Dv^2}{4}=1,$$

即有

$$p_{l-2}=-\widetilde{C}v-\lambda p_{l-1},\ q_{l-1}=\frac{u-v|\widetilde{B}|}{2}-\lambda q_{l-1} \tag{3.76}$$

这里 $\lambda\in\mathbb{Z}$。再由(3.75)、(3.76)及(3.64)—(3.74)有

$$P_l=2\lambda\widetilde{A}+|\widetilde{B}|,$$

$$a_l=\left[\frac{P_l+\sqrt{D}}{2Q_l}\right]=\left[\frac{2\lambda\widetilde{A}+|\widetilde{B}|+\sqrt{D}}{2\widetilde{A}}\right]$$

$$=\lambda+\left[\frac{|\widetilde{B}|+\sqrt{D}}{2\widetilde{A}}\right]=\lambda+a_0,$$

$$P_{l+1}=2a_lQ_l-P_l=2(\lambda+a_0)\widetilde{A}-(2\lambda\widetilde{A}+|\widetilde{B}|)$$
$$=2a_0\widetilde{A}-|\widetilde{B}|=P_1,$$

$$Q_{l+1}=\frac{D-P_{l+1}^2}{4Q_l}=\frac{D-P_1^2}{4Q_0}=Q_1,$$

这就证明了 $k|l$，以及 $a_l=a_k$，也即

$$k|l,\ \lambda=a_k-a_0. \tag{3.77}$$

令 $l=mk$，m 为一个正整数，则有

$$\frac{p_{l-1}}{q_{l-1}}$$

$$=[a_0,\ \underbrace{a_1,\ \cdots,\ a_k,\ a_1,\ \cdots,\ a_k,\ \cdots,\ a_1,\ \cdots,\ a_k}_{\text{共 } m-1 \text{ 组}},a_1,\cdots,a_{k-1}],$$

易见有

$$[0,\ a_1,\ \cdots,\ a_{l-1}]=\frac{p_{l-1}}{q_{l-1}}-a_0,\ [0,\ a_{l-1},\ a_{l-2},\ \cdots,\ a_1]$$
$$=\frac{q_{l-2}}{q_{l-1}},\tag{3.78}$$

由(3.27)和(3.78)得

$$s(p_{l-1},\ q_{l-1})=\frac{-1+(-1)^{l-1}}{8}+\frac{1}{12}([0,\ a_1,\ \cdots,\ a_{l-1}]$$
$$+(-1)^l[0,\ a_{l-1},\ a_{l-2},\ \cdots,\ a_1]+a_1-a_2$$
$$+\cdots+(-1)^l a_{l-1})$$
$$=-\frac{1}{4}+\frac{1}{12}\left(\frac{p_{l-1}}{q_{l-1}}-a_0+\frac{q_{l-2}}{q_{l-1}}\right.$$
$$\left.+\sum_{j=1}^{l-1}(-1)^{j+1}a_j\right)$$
$$=-\frac{1}{4}+\frac{1}{12}\left(\frac{p_{l-1}+q_{l-2}}{q_{l-1}}-a_0\right)$$
$$+\frac{1}{12}\sum_{j=1}^{l-1}(-1)^{j+1}a_j\sum_{n=0}^{m-1}(-1)^{kn}$$
$$+\frac{a_k}{12}\sum^{m-1}(-1)^{kn+1}.\tag{3.79}$$

又由(3.75)、(3.76)与(3.77)有

$$\frac{u}{\widetilde{A}v}=\frac{p_{l-1}+q_{l-2}}{q_{l-1}}+\lambda=\frac{p_{l-1}+q_{l-2}}{q_{l-1}}+a_k-a_0,$$

这样，由定理 1.1、(3.25) 和(3.79)有

$$\Phi\left(\begin{pmatrix}\dfrac{u\pm\widetilde{B}v}{2} & -\widetilde{C}v\\ \widetilde{A}v & \dfrac{u\mp\widetilde{B}v}{2}\end{pmatrix}\right)=\frac{u}{\widetilde{A}v}-12s\left(\frac{u+v|\widetilde{B}|}{2},\ \widetilde{A}v\right)$$

$$=\frac{u}{\widetilde{A}v}-12s(p_{l-1},\ q_{l-1})$$

$$= \frac{p_{l-1}+q_{l-2}}{q_{l-1}} + a_k - a_0 + 3 - \left(\frac{p_{l-1}+q_{l-2}}{q_{l-1}} - a_0\right)$$

$$+ \sum_{j=1}^{l-1}(-1)^j a_j \sum_{n=0}^{m-1}(-1)^{kn} + a_k \sum_{n=1}^{m-1}(-1)^{kn}$$

$$= 3 + \left(a_k + \sum_{j=1}^{k-1}(-1)^j a_j\right)\sum_{n=1}^{m-1}(-1)^{kn}$$

$$= \begin{cases} 3, & \text{如 } k \text{ 奇;} \\ 3 + m\sum\limits_{j=1}^{k}(-1)^j a_j, & \text{如 } k \text{ 偶,} \end{cases}$$

以上用到：如 k 奇，则由 l 偶及 $l=mk$ 知 m 为偶数，从而

$$\sum_{n=0}^{m-1}(-1)^{kn} = 0.$$

这样，我们得到

$$\Phi\left(\begin{pmatrix} \frac{u\pm\tilde{B}v}{2} & -\tilde{C}v \\ \tilde{A}v & \frac{u\mp\tilde{B}v}{2} \end{pmatrix}\right) = 3 + m\Psi\left(\frac{|\tilde{B}|+\sqrt{D}}{2\tilde{A}}\right). \tag{3.80}$$

由

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \frac{u\pm\tilde{B}v}{2} & \tilde{A}v \\ -\tilde{C}v & \frac{u\mp\tilde{B}v}{2} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} \tilde{C}v & \frac{-u\pm\tilde{B}v}{2} \\ \frac{u\pm\tilde{B}v}{2} & \tilde{A}v \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{u\mp\tilde{B}v}{2} & \tilde{C}v \\ -\tilde{A}v & \frac{u\pm\tilde{B}v}{2} \end{pmatrix},$$

及

$$\frac{u\pm\tilde{B}v}{2},\ \tilde{A},\ -\tilde{C},\ v>0,$$

用(3.23)，仿前即得

$$\Phi\left(\left(\begin{matrix}\frac{u\pm\tilde{B}v}{2} & \tilde{A}v\\ -\tilde{C}v & \frac{u\mp\tilde{B}v}{2}\end{matrix}\right)\right)$$

$$=6+\Phi\left(\left(\begin{matrix}\frac{u\mp\tilde{B}v}{2} & \tilde{C}v\\ -\tilde{A}v & \frac{u\pm\tilde{B}v}{2}\end{matrix}\right)\right)$$

$$=6-\left(\frac{u}{\tilde{A}v}-12s\left(\frac{u+|\tilde{B}|v}{2},\ \tilde{A}v\right)\right)$$

$$=3-m\Psi\left(\frac{|\tilde{B}|+\sqrt{D}}{2\tilde{A}}\right). \tag{3.81}$$

于是由(3.57)—(3.59), (3 80)—(3.81)有

$$\Phi(M)=\left(3+\delta m\ \Psi\left(\frac{|\tilde{B}|+\sqrt{D}}{2\tilde{A}}\right)\right)\operatorname{sign}(a+d),\ \text{如 } c>0. \tag{3.82}$$

这里还用了与得到(3.40)相同的推理。

由第一章知道，相应于 $\frac{|\tilde{B}|+\sqrt{D}}{2\tilde{A}}$ 的简单连分数展开式(3.61)，$\frac{-|\tilde{B}|+\sqrt{D}}{2\tilde{A}}$ 的简单连分数展开式为：

$$\frac{|\tilde{B}|+\sqrt{D}}{2\tilde{A}}=[a_k-a_0,\ \overline{a_{k-1}a_{k-2},\ \cdots,\ a_2,\ a_1,\ a_k,}\ ],$$

这里 $\overline{a_{k-1},\ a_{k-2},\ \cdots,\ a_2,\ a_1,\ a_k}$ 为基本周期。

对 k 为奇或偶两种情形，分别讨论后，可知有

$$\Psi\left(\frac{|\tilde{B}|+\sqrt{D}}{2\tilde{A}}\right)=\Psi\left(\frac{-|\tilde{B}|+\sqrt{D}}{2\tilde{A}}\right)$$

$$=\Psi\left(\frac{\delta\tilde{B}+\sqrt{D}}{2\tilde{A}}\right),$$

从而由(3.82)得出

$$\Phi(M)=\left(3+\delta m\Psi\left(\frac{\delta\tilde{B}+\sqrt{D}}{2\tilde{A}}\right)\right)\operatorname{sign}(a+d),\ \text{如 } c>0. \tag{3.83}$$

所以，我们不妨设

$$\frac{\delta\widetilde{B}+\sqrt{D}}{2\widetilde{A}}=[a_0,\overline{a_1,\ \cdots,a_k}],\tag{3.84}$$

其中 $\overline{a_1,\ \cdots,\ a_k}$ 为基本周期。

又由(3.41)—(3.44)易得

$$\frac{\delta r\dfrac{B+\sqrt{D}}{2A}+\delta s}{t\dfrac{B+\sqrt{D}}{2A}+r_1}=\frac{\delta\widetilde{B}+\sqrt{D}}{2\widetilde{A}}$$

及

$$\delta rr_1-\delta st=\delta=\pm1,$$

可知 $\dfrac{B+\sqrt{D}}{2A}$ 的简单连分数展开式

$$\frac{B+\sqrt{D}}{2A}=[\hat{a}_0,\ \hat{a}_1,\ \cdots,\ \hat{a}_n,\ \overline{a_1,\ \cdots,a_k}],\tag{3.85}$$

其基本周期 $\overline{a_1,\cdots,\ a_k}$ 与 $\dfrac{\delta\widetilde{B}+\sqrt{D}}{2\widetilde{A}}$ 的是相同的，并有

$$\delta=(-1)^n.\tag{3.86}$$

这样，由(3.83)—(3.86)即得

$$\begin{aligned}\Phi(M)&=\left(3+m\Psi\left(\frac{B+\sqrt{D}}{2A}\right)\right)\mathrm{sign}(a+d)\\&=\left(3+m\Psi\left(\frac{a-d+\sqrt{(a+d)^2-4}}{2c}\right)\right)\mathrm{sign}(a+d),\\&\qquad 如\ c>0,\end{aligned}\tag{3.87}$$

最后还用到(3.34)—(3.37)。

只要注意到 $\dfrac{-B+\sqrt{D}}{2A}$ 相对于 $\dfrac{-\delta\widetilde{B}+\sqrt{D}}{2\widetilde{A}}$ 的 n 与 $\dfrac{B+\sqrt{D}}{2A}$ 相对于 $\dfrac{\delta\widetilde{B}+\sqrt{D}}{2\widetilde{A}}$ 的 n 显然只差一个偶数，因此我们得到了在说明可设 $c>0$ 时所需要的事实。从而由(3.87)和(3.21)得出

$$\Phi(M)=\left(3+m\Psi\left(\frac{a-d+\sqrt{(a+d)^2-4}}{2|c|}\right)\right)\operatorname{sign}(c(a+d)). \tag{3.88}$$

剩下来只需证明 m 为定理中所描述的。

由于 $k|l$((3.77))，因此有

$$P_k=P_l=2\lambda\widetilde{A}+|\widetilde{B}|,$$

再由 $Q_k=\widetilde{A}$，用(3.65)和(3.66)可得

$$(|\widetilde{B}|p_{k-1}-\widetilde{C}q_{k-1})q_{k-1}\equiv 0(\bmod \widetilde{A}),$$
$$(|\widetilde{B}|p_{k-2}-\widetilde{C}q_{k-2})q_{k-1}\equiv 0(\bmod \widetilde{A}).$$

由此即有

$$|\widetilde{B}|q_{k-1},\ \widetilde{C}q_{k-1}\equiv 0(\bmod \widetilde{A}),$$

再由 $g.c.d.(\widetilde{A},\widetilde{B},\widetilde{C})=1$，即得

$$q_{k-1}\equiv 0(\bmod \widetilde{A}).$$

命有理整数 u_1, v_1，使

$$q_{k-1}=\widetilde{A}v_1,\ u_1=2p_{k-1}-|\widetilde{B}|v_1,$$

则有

$$\begin{aligned}u_1^2-Dv_1^2&=4p_{k-1}^2-4|\widetilde{B}|v_1p_{k-1}+\widetilde{B}^2v_1^2-Dv_1^2\\&=\frac{4}{\widetilde{A}}(\widetilde{A}p_{k-1}^2-|\widetilde{B}|p_{k-1}q_{k-1}+\widetilde{C}q_{k-1}^2)\\&=\frac{4}{\widetilde{A}}(-1)^kQ_k=(-1)^k4,\end{aligned} \tag{3.89}$$

其中还用到(3.65)。这样当 k 奇时，不定方程

$$x^2-Dy^2=-4,\ x,\ y\in\mathbb{Z} \tag{3.90}$$

有解，这时不必顾及 m 是什么值了，因为这时有

$$\Psi\left(\frac{a-d+\sqrt{(a+d)^2-4}}{2a}\right)=0.$$

反之，如(3.90)有解，即存在正整数 u_2, v_2，使 $u_2^2-Dv_2^2=-4$. 令

$$q=\widetilde{A}v_2,\quad p=\frac{u_2+|\widetilde{B}|v_2}{2},$$

则 p、q 是正整数，且有

$$p\frac{u_2-|\widetilde{B}|v_2}{2}+q\widetilde{C}v_2=\frac{u_2^2-Dv_2^2}{4}=-1.$$

从而得到 $g.c.d.(p, q)=1$, 以及

$$\widetilde{A}p^2-|\widetilde{B}|pq+\widetilde{C}q^2=-\widetilde{A}.$$

由此及 $0<\widetilde{A}<\frac{\sqrt{D}}{2}$, 用第一章的结果, 即知 $\frac{p}{q}$ 是 $\frac{|\widetilde{B}|+\sqrt{D}}{2\widetilde{A}}$ 的一个渐近分数, 即存在正整数 $l_1\geqslant 1$, 使

$$p=p_{l_1-1},\ q=q_{l_1-1},\ (-1)^{l_1}Q_{l_1}=-\widetilde{A}.$$

由此即知 l_1 为奇数, 且 $Q_{l_1}=\widetilde{A}$. 仿照上面的方法, 可得到 $k|l_1$, 于是 k 为奇数。这就给出了列于证明之后的附注。

当 k 为偶数时, 由上面所证明的有

$$q_{k-1}=\widetilde{A}v_1,\ p_{k-1}=\frac{u_1+|\widetilde{B}|v_1}{2},$$

$$q_{l-1}=\widetilde{A}v_1,\ p_{l-1}=\frac{u+|\widetilde{B}|v}{2},\ l=mk, \tag{3.91}$$

并且 u_1, v_1, u, v 均为正整数, l 与 k 为偶数。

由(3.91)有

$$\frac{u_1+\sqrt{D}v_1}{2}=p_{k-1}-\omega' q_{k-1},$$

$$\frac{u+\sqrt{D}v}{2}=p_{l-1}-\omega' q_{l-1}. \tag{3.92}$$

这里

$$\omega'=\frac{|\widetilde{B}|-\sqrt{D}}{2\widetilde{A}},\ \omega=\frac{|\widetilde{B}|+\sqrt{D}}{2\widetilde{A}}. \tag{3.93}$$

由第一章的结果可知, $p_{k-1}-\omega' q_{k-1}$ 是 Pell 方程

$$x^2-Dy^2=4,\ x,\ y\in\mathbb{Z} \tag{3.94}$$

的基本解。故由(3.92)知 $\frac{u_1+\sqrt{D}v_1}{2}$ 是(3.94)的基本解。

我们来证明

$$\frac{u+\sqrt{D}v}{2}=\left(\frac{u_1+\sqrt{D}v_1}{2}\right)^m, \tag{3.95}$$

由此即可完成我们对定理的证明。

我们对m行归纳法来证明(3.95)。

当$m=1$时，由(3.91)有$l=k$，由(3.92)知(3.95)显然成立。

假定(3.95)对$m\geqslant 1$已成立，即已有

$$p_{mk-1}-\omega' q_{mk-1}=(p_{k-1}-\omega' q_{k-1})^m. \tag{3.96}$$

由(注意k为偶数)

$$\begin{aligned}\widetilde{A}&=(-1)^{mk}\widetilde{A}=(-1)^{mk}Q_{km}=\widetilde{A}p_{mk-1}^2-|\widetilde{B}|p_{mk-1}q_{mk-1}\\&\quad+\widetilde{C}q_{mk-1}^2,\quad -(2(a_k-a_0)\widetilde{A}+\widetilde{B})=(-1)^{mk-1}p_{mk}\\&=2\widetilde{A}p_{mk-1}p_{mk-2}-|\widetilde{B}|(p_{mk-1}q_{mk-2}+p_{mk-2}q_{mk-1})\\&\quad+2\widetilde{C}q_{mk-1}q_{mk-2}.\end{aligned}$$

即得

$$p_{mk-1}-\frac{\widetilde{B}}{\widetilde{A}}q_{mk-1}-(a_k-a_0)q_{mk-1}-q_{mk-2}=0,$$

$$\frac{\widetilde{C}}{\widetilde{A}}q_{mk-1}+(a_k-a_0)p_{mk-1}+p_{mk-2}=0,$$

由此，再用$\widetilde{A}\omega'^2-|\widetilde{B}|\omega'+\widetilde{C}=0$(注意(3.93))，即有

$$\begin{aligned}&(a_k-a_0+\omega')(p_{mk-1}-\omega' q_{mk-1})+(p_{mk-2}-\omega' q_{mk-2})\\&=\frac{\widetilde{C}}{\widetilde{A}}q_{mk-1}+(a_k-a_0)p_{mk-1}+p_{mk-2}\\&\quad+\omega'\left(p_{mk-1}-(a_k-a_0)q_{mk-1}-\frac{|\widetilde{B}|}{\widetilde{A}}q_{mk-1}-q_{mk-2}\right)=0,\end{aligned}$$

即有

$$(a_k-a_0+\omega')(p_{mk-1}-\omega' q_{mk-1})+(p_{mk-2}-\omega' q_{mk-2})=0, \tag{3.97}$$

由

$$[a_k,\ a_1,\ \cdots,\ a_{k-1}]=a_k-a_0+\frac{p_{k-1}}{q_{k-1}},$$

即有

$$\frac{p_{(m+1)k-1}}{q_{(m+1)k-1}}=\left[a_0,\ a_1,\ \cdots,\ a_{mk-1},\ \frac{p_{k-1}}{q_{k-1}}+a_k-a_0\right]$$

$$= \frac{\left(a_k - a_0 + \frac{p_{k-1}}{q_{k-1}}\right) p_{mk-1} + p_{mk-2}}{\left(a_k - a_0 + \frac{p_{k-1}}{q_{k-1}}\right) q_{mk-1} + q_{mk-2}},$$

于是有

$$\begin{aligned} p_{(m+1)k-1} - \omega' q_{(m+1)k-1} &= p_{k-1}(p_{mk-1} - \omega' q_{mk-1}) \\ &\quad + q_{k-1}(p_{mk-2} - \omega' q_{mk-2} + (a_k - a_0)(p_{mk-1} - \omega' q_{mk-1})) \\ &= (p_{k-1} - \omega' q_{k-1})(p_{mk-1} - \omega' q_{mk-1}) \\ &\quad + q_{k-1}(p_{mk-2} - \omega' q_{mk-2} + (a_k - a_0 + \omega')(p_{mk-1} - \omega' q_{mk-1})) \\ &= (p_{k-1} - \omega' q_{k-1})(p_{mk-1} - \omega' q_{mk-1}), \end{aligned} \tag{3.98}$$

最后一步用了(3.97)，由归纳假设(3.96)和(3.98)即有

$$p_{(m+1)k-1} - \omega' q_{(m+1)k-1} = (p_{k-1} - \omega' q_{k-1})^{m+1},$$

即(3.95)在$m+1$时也成立。完成了归纳法证明，定理得证。

证明中关于k为奇时的论断，给出了下面的附注

附注 Ψ定义中的简单连分数展开式周期的长度k为奇数的充要条件是负Pell方程

$$x^2 - Dy^2 = -4, \ x, \ y \in \mathbb{Z}$$

有解。

推论 设h, k为两个正整数，$g.c.d.(h, k) = 1$。再设正整数h'满足$hh' \equiv 1 \pmod{k}$。如$h + h' > 2$，则Dedekind和

$$s(h, k) = s(h', k) = \begin{cases} \dfrac{h+h'}{12k} - \dfrac{1}{4}, & \text{如} r \text{奇；} \\ \dfrac{h+h'}{12k} - \dfrac{1}{4} - \dfrac{m}{12} \sum_{j=1}^{r} (-1)^{n+j} a_j, & \text{如} r \text{偶，} \end{cases}$$

这里的r是简单连分数展开式

$$\frac{h - h' + \sqrt{(h+h')^2 - 4}}{2k} = [\hat{a}_0, \hat{a}_1, \cdots, \hat{a}_n, \overline{a_1, \cdots, a_r}]$$

的基本周期$\overline{a_1, \cdots, a_r}$的长度，而正整数$m$定义如下。令

$$u = h + h', \quad v = g.c.d.\left(h - h', \ k, \ \frac{hh' - 1}{k}\right),$$

$$D = v^{-2}(u^2 - 4),$$

则D是一个非完全平方的正整数，并有

$$\frac{u+v\sqrt{D}}{2}=\left(\frac{u_0+v_0\sqrt{D}}{2}\right)^m,$$

其中 Pell 方程

$$x^2-y^2D=4,\ x,\ y\in\mathbf{Z}$$

的基本解是

$$\frac{u_0+v_0\sqrt{D}}{2}.$$

1.3 Hurwitz ζ-函数

对满足 $0<u\leqslant 1$ 的实数，定义 Hurwitz ζ-函数为

$$\zeta(s,u)=\sum_{n=0}^{\infty}\frac{1}{(n+u)^s},\ \mathrm{Re}\,s>1.$$

$\zeta(s,1)=\zeta(s)$ 即为 Riemann ζ-函数。$\zeta(s,u)$ 可以解析开拓到整个 s 平面，成为 s 的一个半纯函数，它仅在 $s=1$ 处有一个一阶极点，除此以外，它都是解析的，并有

$$\zeta(s,u)=\frac{1}{s-1}-\psi(u)+O(|s-1|),\ s\to 1, \tag{3.99}$$

这里 $\psi(u)$ 是 Γ-函数 $\Gamma(u)$ 的对数微商，即有

$$\psi(u)=\frac{\Gamma'(u)}{\Gamma(u)},\ 0<u\leqslant 1.$$

注意 $\psi(1)=-\gamma$，$\gamma=0.57721566490\cdots$ 是 Euler 常数。

存在一个 s 的整函数

$$H_u(s)=\int_C\frac{z^{s-1}e^{uz}}{e^z-1}dz$$

(其中围道 C 为从 $-\infty$ 沿负下半实轴到绕过原点附近的一个小圆，再沿负上半实轴回到 $-\infty$) 使

$$-2\pi i\zeta(s,u)=\Gamma(1-s)H_u(s),$$

并且

$$H_u(s)=-(2\pi)^s\sum_{n=1}^{\infty}\frac{2i\sin\left(2\pi un+\frac{s}{2}\pi\right)}{n^{1-s}},\ \mathrm{Re}\,s<0. \tag{3.100}$$

上述知识可见之于S.Lang《Introduction to Modular Forms》第14章。本小节其余部分致力于证明下列的定理。

定理 1.3　设 d 为基本判别式，$f(x, y)=ax^2+bxy+cy^2$ 是判别式 $d=b^2-4ac$ 的二元二次原型。χ 为 mod k 的原特征，这里 k 是一个正整数，那么我们有：

(1) 当 χ 为mod k 的实原特征，且为 $\mathscr{C}_0(d)$（即判别式为 d 的二元二次原型类群）的一个 genus 特征，同时满足 $g.c.d.(a, d)=1$ 时，则有

$$\frac{1}{k\varphi(k)}\sum_{1\leqslant m,n\leqslant k}\chi(f(m, n))\psi\left(\frac{n}{k}\right)=-\chi(f)(\gamma+\log k),$$

这里 $\varphi(k)$ 为 Euler 函数，γ 为 Euler 常数；

(2) 当 χ 为 mod p 的原特征，这里 p 为一个奇素数，$p|d$，并且 $\chi\neq\rho$，而 ρ 是 mod p 的 Legendre 符号，则有

$$\sum_{1\leqslant m,n\leqslant p}\chi(f(m, n))\psi\left(\frac{n}{p}\right)=\begin{cases}0, & \text{当 } p\nmid a;\\ -p^2\chi(c)L(1, \chi^2), & \text{当 } p|a;\end{cases}$$

(3) 当 χ 为 mod p 的原特征，这里 p 为一个奇素数，$p\nmid a$，ρ 的定义同(2)，则有

$$\begin{aligned}&\sum_{1\leqslant m,n\leqslant p}\chi(f(m, n))\psi\left(\frac{n}{p}\right)\\&=\begin{cases}\chi(a)p\log p, & \text{当}\chi=\rho;\\ -\bar{\chi}(4a)\chi(-d)\rho(d)pL(1, \chi^2)J(\chi, \rho), & \text{当}\chi\neq\rho;\end{cases}\end{aligned}$$

这里 $J(\chi, \rho)$ 是 Jacobi 和

$$J(\chi, \rho)=\sum_{\substack{m_1, m_2(\bmod p)\\ m_1+m_2\equiv 1(\bmod p)}}\chi(m_1)\rho(m_2);$$

(4) 当 χ 为 mod k 的实原特征，且 $g.c.d.(k, d)=1$ 时，则有

$$\sum_{1\leqslant m,n\leqslant k}\chi(f(m,n))\psi\left(\frac{n}{k}\right)=\begin{cases}0, \text{如 } k \text{ 至少有两个不同的素因子；}\\ \chi(a)k\log p, \text{如 } k \text{ 为一个素数 } p \text{ 的幂。}\end{cases}$$

我们提醒一下，$d<0$ 时，我们只考虑正定型。

为证明定理，先给出下面的引理。

引理 1.1　我们有

$$\sum_{m=0}^{n-1} \psi\left(\frac{m}{n}+z\right)=n\psi(nz)-n\log n,$$

只要等式两边都有意义。

证明 这是一个熟知的事实，参见任何有关Γ函数的书。

引理1.2 设 k 为一个正整数，对一个 mod k 的特征 χ，有

$$\sum_{n=1}^{k}\chi(n)\psi\left(\frac{n}{k}\right)=\begin{cases}-kL(1,\chi), & \text{如}\chi\text{是}\bmod k\text{非主特征；}\\ -\left(\gamma+\log k+\sum\limits_{p\mid k}\dfrac{\log p}{p-1}\right)\varphi(k), & \text{如}\chi\text{为主特征，}\end{cases}$$

p 表素数。

证明 当 χ 为 mod k 的主特征时，用 μöbius 函数 μ 可得

$$\sum_{n=1}^{k}\chi(n)\psi\left(\frac{n}{k}\right)=\sum_{1\leqslant n\leqslant k}\psi\left(\frac{n}{k}\right)\sum_{1\leqslant m\mid n,k}\mu(m)$$

$$=\sum_{1\leqslant m\mid k}\mu(m)\sum_{1\leqslant n\leqslant\frac{k}{m}}\psi\left(\frac{n}{k/m}\right)\text{(用引理 3.1, 可得)}$$

$$=\sum_{1\leqslant m\mid k}\mu(m)\ \frac{k}{m}\left(\psi(1)-\log\frac{k}{m}\right)$$

$$=-k(\gamma+\log k)\sum_{1\leqslant m\mid k}\frac{\mu(m)}{m}+k\sum_{1\leqslant m\mid k}\frac{\mu(m)\log m}{m}$$

$$=-\left(\gamma+\log k+\sum_{p\mid k}\frac{\log p}{p-1}\right)\varphi(k),$$

p 表素数。

当 χ 为 mod k 的非主特征时，由(3.99)即有

$$\sum_{m=1}^{k}\chi(m)\psi\left(\frac{m}{k}\right)=\frac{1}{s-1}\sum_{m(\bmod k)}\chi(m)$$

$$-\sum_{1\leqslant m\leqslant k}\sum_{n=0}^{\infty}\frac{\chi(m)}{\left(n+\frac{m}{k}\right)^{s}}+O(|s-1|),\text{ 当 } s\to 1.$$

上面的右边的第一个和是零，因为 χ 是 mod k 非主特征，第二个和是

$$k^{s}\sum^{\infty}\frac{\chi(n)}{n^{s}}=kL(1,\chi)+O(|s-1|),\text{ 当 } s\to 1.$$

于是得到所需。引理证毕。

定理 1.3 的证明

(1) 此时，χ 是 $\mathscr{C}_0(d)$ 的一个 genus 特征。我们首先指出，由于 $g.c.d.(a,\ d)=1$，由 genus 特征的定义可知有 $\chi(f)=\chi(a)$。并且 $\chi_d(*)=\left(\frac{d}{*}\right)$(Kronecker 符号)可分解为

$$\chi_d=\chi\chi_1,$$

其中 χ_1 为 mod k_1 的实原特征，$|d|=kk_1$，$g.c.d.(k,\ k_1)=1$。

我们先来看 $\pm k$ 为素判别式，即 $\pm k=\pm$ 奇素数 p，-4，± 8，而 $\chi=\rho$(mod$p$ Legendre 符号)，$\left(\frac{-4}{*}\right)$，$\left(\frac{\pm 8}{*}\right)$ (这两者均为 Kronecker 符号)的情形。

当 $k=$ 奇素数 p，而 $\chi=\rho$ 时，

$$\begin{aligned}
&\sum_{1\leqslant m,n\leqslant p}\chi(f(m,\ n))\psi\left(\frac{n}{p}\right)\\
&=\chi(4a)\sum_{1\leqslant m,n\leqslant p}\chi((2am+bn)^2-dn^2)\,\psi\left(\frac{n}{p}\right)\\
&=\chi(a)\sum_{n=1}^{p}\psi\left(\frac{n}{p}\right)\sum_{m(\mathrm{mod}\ p)}\chi^2(m)\\
&=\chi(a)(p-1)p(\psi(1)-\log p)=-\chi(f)k\varphi(k)(\gamma+\log k),
\end{aligned}$$

即此时断言成立。

当 $k=4$，而 $\chi(*)=\left(\frac{-4}{*}\right)$(Kronecker 符号)时，有 $4|d$ 且 $\frac{d}{4}\equiv 3(\mathrm{mod}4)$，$a$ 奇，$a^2\equiv 1(\mathrm{mod}\ 8)$，$b$ 偶，$b=2b_1$，$b_1^2-ac\equiv 3(\mathrm{mod}\ 4)$。于是

$$\begin{aligned}
&\sum_{1\leqslant m,n\leqslant 4}\chi(f(m,\ n))\psi\left(\frac{n}{4}\right)\\
&=\left(\frac{-4}{a}\right)\sum^{4}\psi\left(\frac{n}{4}\right)\sum_{m(\mathrm{mod}\ 4)}\left(\frac{-4}{a^2m^2+2ab_1mn+acn^2}\right)\\
&=\left(\frac{-4}{a}\right)\sum^{4}\psi\left(\frac{n}{4}\right)\sum_{m(\mathrm{mod}\ 4)}\left(\frac{-4}{m^2+n^2}\right)\\
&=2\left(\frac{-4}{a}\right)\sum^{4}\psi\left(\frac{n}{4}\right)=-8\left(\frac{-4}{a}\right)(\gamma+\log 4)\\
&=-\chi(f)k\varphi(k)(\gamma+\log k),
\end{aligned}$$

即此时断言成立。

当 $k=8$，而 $\chi(*)=\left(\frac{\pm 8}{*}\right)$(Kronecker 符号)时，有 $4|d$ 且 $\frac{d}{4}\equiv 2(\mathrm{mod}\,4)$，$a$ 奇，$a^2\equiv 1(\mathrm{mod}\,8)$，$b$ 偶，$b=2b_1$，$b_1^2-ac\equiv 2(\mathrm{mod}\,4)$。于是

$$\begin{aligned}&\sum_{1\le m,n\le 8}\chi(f(m,n))\psi\left(\frac{n}{8}\right)\\&=\left(\frac{\pm 8}{a}\right)\sum^{8}\psi\left(\frac{n}{8}\right)\sum_{(\mathrm{mod}\,8)}\left(\frac{\pm 8}{m^2a^2+2ab_1mn+acb^2}\right)\\&=\left(\frac{\pm 8}{a}\right)\sum^{8}\psi\left(\frac{n}{8}\right)\sum_{m(\mathrm{mod}\,8)}\left(\frac{\pm 8}{m^2+(ac-b_1^2)n^2}\right),\end{aligned}\qquad(3.101)$$

易见上式的内和

$$=\begin{cases}4, & \text{当 } n \text{ 为偶数;}\\ 4\left(\frac{\pm 8}{1+ac-b_1^2}\right), & \text{当 } n \text{ 为奇数,}\end{cases}\qquad(3.102)$$

因此

当 n 为偶数时，用 $\left(\frac{\pm 8}{a}\right)=\chi(f)$，

当 n 为奇数，而 b_1 奇时，c 也奇，用

$$\left(\frac{\pm 8}{a}\right)\left(\frac{\pm 8}{1+ac-b_1^2}\right)=\left(\frac{\pm 8}{a}\right)\left(\frac{\pm 8}{ac}\right)=\left(\frac{\pm 8}{c}\right)=\chi(f),$$

当 n 为奇数，而 b_1 偶时，c 也偶，且显然有 $a+a^2c-ab_1^2\equiv a+a^2c-ab_1^2\equiv a+b+c(\mathrm{mod}\,8)$，用

$$\left(\frac{\pm 8}{a}\right)\left(\frac{\pm 8}{1+ac-b_1^2}\right)=\left(\frac{\pm 8}{a+a^2c-ab_1^2}\right)=\left(\frac{\pm 8}{a+b+c}\right)$$
$$=\chi(f),$$

由(3.101)和(3.102)可得

$$\sum_{1\le m,n\le 8}\chi(f(m,n))\psi\left(\frac{n}{8}\right)=4\chi(f)\sum_{n=1}^{8}\psi\left(\frac{n}{8}\right)=-\chi(f)k\varphi(k)(\gamma+\log k).$$

这样证明了，当 k 只有一个素因子时，断言成立。以下对 k 的素因子个数用归纳法来证明断言是成立的。

如 k 至少有两个素因子，则 k 至少有一个奇素因子 p，而且有 $k=k_1p$，$p\nmid k_1$，$p\|d$，$k_1|d$。令 $m=pm_1+k_1m_2$。又 χ 可分

解为 $\chi_1\chi_2$，其中 χ_1 为 $\bmod k_1$ 的实原特征，$\chi_2=\rho$（即 $\bmod p$ 的 Legendre 符号），并且 χ_1，χ_2 均为 $\mathscr{C}_0(d)$ 的 genus特征。

于是

$$\sum \overset{\text{def}}{=} \sum_{1\leqslant m,n\leqslant k} \chi(f(m,n))\psi\left(\frac{n}{k}\right)$$

$$= \sum_{1\leqslant n\leqslant k} \psi\left(\frac{n}{k}\right) \sum_{m_1(\bmod k_1)} \chi_1(f(pm_1,n)) \sum_{m_2(\bmod p)} \chi_2(f(k_1m_2,n))$$

$$= \sum_{1\leqslant n\leqslant k} \psi\left(\frac{n}{k}\right) \sum_{m_1(\bmod k_1)} \chi_1(f(m_1,n)) \sum_{m_2(\bmod p)} \chi_2(f(m_2,n))$$

$$= \chi_2(4a) \sum_{1\leqslant n\leqslant k} \psi\left(\frac{n}{k}\right) \sum_{m_1(\bmod k_1)} \chi_1(f(m_1,n)) \sum_{m_2(\bmod p)} \chi_2(m_2^2-dn^2)$$

$$= \chi_2(a)(p-1) \sum_{1\leqslant n\leqslant k} \psi\left(\frac{n}{k}\right) \sum_{m_1(\bmod k_1)} \chi_1(f(m,n)),$$

令 $n=k_1n_1+n_2$，$0\leqslant n_1\leqslant p-1$，$1\leqslant n_2\leqslant k_1$，即有

$$\sum = \chi_2(a)(p-1) \sum_{1\leqslant m,n\leqslant k_1} \chi_1(f(m,n)) \sum_{n_1=0}^{p-1} \psi\left(\frac{n_1}{p}+\frac{n}{k}\right)$$

$$= \chi_2(a)(p-1)p \sum_{1\leqslant m,n\leqslant k_1} \chi_1(f(m,n))\psi\left(\frac{n}{k_1}\right)$$

$$-\chi_2(a)(p-1)p\log p \sum_{m,n(\bmod k_1)} \chi_1(f(m,n)),$$

对第一个和用归纳假设，而对第二个和用第二章定理1.8，即得

$$\begin{aligned}\sum = & -\chi_2(f)p\varphi(p)\chi_1(f)k_1\varphi(k_1)(\gamma+\log k_1)\\ & -\chi_2(f)p\varphi(p)k_1\varphi(k_1)\chi_1(f)\log p\\ = & -\chi(f)k\varphi(k)(\gamma+\log k),\end{aligned}$$

其中用到 $\chi_1(f)\chi_2(f)=\chi(f)$。

这样归纳步骤完成，因此断言(1)已证明。

(2) 当 $p\nmid a$ 时，由 $p\mid d$ 即知

$$\sum_{1\leqslant m,n\leqslant p} \chi(f(m,n))\psi\left(\frac{n}{p}\right) = \sum_{n=1}^{p} \psi\left(\frac{n}{p}\right)\bar{\chi}(4a) \sum_{m(\bmod p)} \chi(m^2-dn^2)$$

$$= \bar{\chi}(4a)\sum_{n=1}^{p} \psi\left(\frac{n}{p}\right) \sum_{m(\bmod p)} \chi^2(m) = 0,$$

这是因为 $\chi\neq\rho$，χ^2 不是主特征。

当 $p\mid a$ 时，由 $p\mid d$ 可知，$p\mid b$，$p\nmid c$。于是

$$\sum_{1<m,n<p}\chi(f(m,n))\psi\left(\frac{n}{p}\right)=p\chi(c)\sum_{n=1}^{p}\chi^2(n)\psi\left(\frac{n}{p}\right)$$

$$=-p^2\chi(c)L(1,\chi^2).$$

其中用到引理1.2。这样，断言(2)已证明。

(3) 当 $p|a$ 时，由 $p\nmid d$，即有 $p\nmid b$，故

$$\sum_{1<m,n<p}\chi(f(m,n))\psi\left(\frac{n}{p}\right)$$

$$=\sum_{n=1}^{p}\psi\left(\frac{n}{p}\right)\sum_{m(\bmod p)}\chi(bnm+cn^2)=0,\quad 如\ p|a. \tag{3.103}$$

这是因为内和为零：当 $p|n$ 时，内和中的每一项都是0，而 $p\nmid n$ 时，整个内和为0。

当 $p\nmid a$ 时，有

$$\sum_{1<m<p}\chi(f(m,n))=\bar{\chi}(4a)\sum_{m(\bmod p)}\chi(m^2-dn^2)$$

$$=\bar{\chi}(4a)\cdot\begin{cases}\chi^2(n)\sum\limits_{m(\bmod p)}\chi(m^2-d), & 当\ p\nmid n;\\ \sum\limits_{m(\bmod p)}\chi^2(m), & 当\ p|n,\end{cases}$$

由此即知，有

$$\sum\overset{\text{def}}{=\!=}\sum_{1<m,n<p}\chi(f(m,n))\psi\left(\frac{n}{p}\right)$$

$$=\bar{\chi}(4a)\psi(1)\sum_{m(\bmod p)}\chi^2(m)$$

$$+\bar{\chi}(4a)\sum_{m(\bmod p)}\chi(m^2-d)\sum_{n=1}^{p}\chi^2(n)\psi\left(\frac{n}{p}\right), \tag{3.104}$$

当 $\chi=\rho$ 时，χ^2 是主特征，故(3.104)的第一项是

$$\bar{\chi}(4a)\psi(1)(p-1),$$

第二项是

$$\bar{\chi}(4a)(p-1)\left(\gamma+\frac{p}{p-1}\log p\right),$$

从而

$$\sum=\chi(a)p\log p,\quad 如\ p\nmid a,\ 且\ \chi=\rho, \tag{3.105}$$

当 $\chi\neq\rho$ 时，χ^2 不是主特征，故(3.104)的第一项是0，对第二项用

$$\sum_{m(\bmod p)}{}' \chi(m^2-d)=\begin{cases}-1, & \text{如 } \chi=\rho, \text{ 且 } p\nmid d;\\ \chi(-d)\rho(d)J(\chi,\rho), & \text{如 } \chi\neq\rho, \text{ 且 } p\nmid d,\end{cases}$$

(其中 $J(\chi,\rho)$是 Jacobi 和)，并用引理 1.2，即有

$$\sum=-\bar{\chi}(4a)\chi(-d)\rho(d)pL(1,\chi^2)J(\chi,\rho),$$

$$\text{如 } p\nmid a, \text{ 且 } \chi\neq\rho, \tag{3.106}$$

由(3.103)、(3.105)和(3.106)，即知断言(3)已证明。

(4) 如 k 至少有两个不同的素因子，则 k 至少有一个奇素因子 p，于是 $k=k_1p$, $k_1>1$, $p\nmid k_1$, 且有 $p\nmid d$, $g.c.d.(d,k_1)=1$。χ 可分解为 $\chi=\chi_1\chi_2$，其中 χ_1 为 mod k_1 的实原特征，χ_2 为mod p 的实原特征，即 $\chi_2=\rho$(mod p 的 Legendre 符号)。令 $m=pm_1+k_1m_2$，即有

$$\sum\overset{\text{def}}{=\!=}\sum_{1\leqslant m,n\leqslant k}\chi(f(m,n))\psi\left(\frac{n}{k}\right)$$

$$=\sum_{n=1}^{k}\psi\left(\frac{n}{k}\right)\sum_{m_1(\bmod k_1)}\chi(f(m_1,n))\sum_{m_2(\bmod p)}\chi_2(f(m_2,n)), \tag{3.107}$$

当 $p|a$ 时，由 $p\nmid d$，有 $p\nmid b$，故(3.107)的内和为0；而当 $p\nmid a$时，(3.107)的内和

$$=\chi_2(4a)\sum_{m_2(\bmod p)}\chi_2(m^2-dn^2)=\chi_2(a)\cdot\begin{cases}-1, & \text{当 } p\nmid n;\\ p-1, & \text{当 } p|n,\end{cases}$$

于是有

$$\sum=-\chi_2(a)\sum_{n=1}^{k}\psi\left(\frac{n}{k}\right)\sum_{m(\bmod k_1)}\chi_1(f(m,n))$$

$$+p\chi_2(a)\sum_{\substack{n=1\\ p|n}}^{k}\psi\left(\frac{n}{k}\right)\sum_{m(\bmod k_1)}\chi_1(f(m,n)), \text{若 } p|a. \tag{3.108}$$

在(3.108)的第一个项中，令 $n=k_1n_1+n_2$, $0\leqslant n_1\leqslant p-1$, $1\leqslant n_2\leqslant k_1$，即知(3.108)的第一项等于

$$-\chi_2(a)p\sum_{1\leqslant m,n\leqslant k_1}\chi_1(f(m,n))\left(\psi\left(\frac{n}{k_1}\right)-\log p\right)$$

而(3.108)的第二项，由于 χ_1 为实原特征且 $p\nmid k_1$，即知它等于

$$\chi_2(a)p\sum_{1\leqslant m,n\leqslant k_1}\chi_1(f(m,n))\psi\left(\frac{n}{k_1}\right).$$

于是有

$$\sum = \chi_2(a)\, p \log p \sum_{m, n (\bmod k_1)} \chi_1(f(m, n)) = 0,$$

这里用到第二章的定理 1.8。

因此断言(4)的第一部分已证明。

以下来看 k 为素数幂的情况，这只有 k 为奇素数 p, 4, 8, 而 $\chi=\rho$, $\chi(*)=\left(\frac{-4}{*}\right)$或$\left(\frac{\pm 8}{*}\right)\left(\rho, \left(\frac{-4}{*}\right), \left(\frac{\pm 8}{*}\right)\text{定义同前}\right)$这四种情形。第一种情形即为断言(3)的第一种情形，以下看 $k=4$ 或 8 时的情形。

$k=4$, $\chi(*)=\left(\frac{-4}{*}\right)$(Kronecher 符号) 时，这时 d 奇，b 也奇。于是当 a 偶时，有

$$\sum_{m (\bmod 4)} \left(\frac{-4}{f(m, n)}\right) = \left(\frac{-4}{Cn^2}\right) + \left(\frac{-4}{a+bn+cn^2}\right)$$
$$+\left(\frac{-4}{2bn+cn^2}\right) + \left(\frac{-4}{a+3bn+cn^2}\right) = 0,$$

这是因为：n 偶时，每一项都是 0；n 奇时，第一项与第三项之和，第二项与第四项之和，均为 0。

因此 a 偶时

$$\sum_{1<m, n<4} \chi(f(m, n)) \psi\left(\frac{n}{4}\right) = 0.$$

当 a 奇时，由于 b 也奇，所以

$$\sum_{m (\bmod 4)} \left(\frac{-4}{f(m, n)}\right) = \left(\frac{-4}{a}\right) \sum_{m (\bmod 4)} \left(\frac{-4}{m^2+abmn+acn^2}\right)$$
$$= \left(\frac{-4}{a}\right) \cdot \begin{cases} 0, & \text{如 } n \text{ 奇;} \\ 2(-1)^{\frac{n}{2}}, & \text{如 } n \text{ 偶,} \end{cases}$$

因此 a 奇时

$$\sum_{1<m, n<4} \chi(f(m, n)) \psi\left(\frac{n}{4}\right) = 2\left(\frac{-4}{a}\right) \sum_{n=1,2} (-1)^n \psi\left(\frac{n}{2}\right)$$
$$= 4\left(\frac{-4}{a}\right) \log 2.$$

这就证明了 $k=4$ 时，断言(4)成立。

$k=8$, $\chi(*)=\left(\frac{\pm 8}{*}\right)$(Kronecker 符号)时，$d$ 奇，b 也奇，从而与 $k=4$ 时一样，可以证明，当 a 偶时，所求的和是 0；而当 a 奇时，类似的有

$$\sum_{m(\bmod 8)}\left(\frac{\pm 8}{f(m,n)}\right)=\left(\frac{\pm 8}{a}\right), \quad \begin{cases}4(-1)^{\frac{n}{4}}, & \text{当 } 4\mid n;\\ 0, & \text{否则},\end{cases}$$

因此

$$\sum_{1<m,n<8}\chi(f(m,n))\psi\left(\frac{n}{8}\right)=4\left(\frac{\pm 8}{a}\right)\sum_{n=1,2}(-1)^n\psi\left(\frac{n}{2}\right)$$
$$=8\left(\frac{\pm 8}{a}\right)\log 2,$$

即 $k=8$ 时断言(4)仍成立。

这样断言(4)已证明。

综上所述，定理已被完全证明。

§2 Kronecker极限公式

2.1 经典的极限公式

在域 K 的理想类 A^{-1} 中取定一个整理想 $\mathfrak{B}$，则映射

$$\mathfrak{A}\mapsto\mathfrak{A}\mathfrak{B}=[\lambda]$$

是由理想类 A 所含的整理想集合到能被 $\mathfrak{B}$ 除尽的主整理想 $[\lambda]$(即 $\lambda\in\mathfrak{B}$) 集合的一个双射(bijection)。又 λ_1, $\lambda_2\in\mathfrak{B}$ 确定同一个主整理想，当且仅当 $\varepsilon\in U_K$(K 的单位群)使 $\lambda_1=\varepsilon\lambda_2$，即当且仅当它们在 $\mathfrak{B}/U_K$ 中有相同的象。因此有

$$\zeta_K(s\mid A)=\sum_{\mathfrak{A}\in A}\frac{1}{N(\mathfrak{A})^s}=N(\mathfrak{B})^s\sum_{\mathfrak{A}\in A}\frac{1}{N(\mathfrak{A}\mathfrak{B})^s}$$
$$=N(\mathfrak{B})^s\sum_{\lambda\in\mathfrak{B}/U_K}{}'\frac{1}{|N(\lambda)|^s},\quad \mathrm{Re}\,s>1, \tag{3.109}$$

这里及以后，求和号上的"$'$"表示略去使分母取值零的那些项。

现设 $K=Q(\sqrt{d})$ 为一个虚的二次域，即 K 的判别式 $d<0$。则 U_K 是一个有限群，其阶 $w_K=2$, 4, 6, 分别相应于 $d<-4$

$d=-4$, $d=-3$。因此由(3.109)得到

$$\zeta_K(s\mid A)=\frac{N(\mathfrak{B})^s}{w_K}\sum_{\lambda\in\mathfrak{B}}{}' N(\lambda)^{-s},\ \mathrm{Re}\,s>1,\ \text{如}K\text{为虚二次域。} \tag{3.110}$$

这里用到在虚二次域中，显然有 $N(\lambda)=\lambda\sigma(\lambda)=\lambda\bar{\lambda}=|\lambda|^2>0$ 的事实。(3.110) 不因以 $\alpha\mathfrak{B}$ 代替 $\mathfrak{B}$ 而改变，只要 $\alpha\in K^*$，因此，可取 $\mathfrak{B}$ 为分式理想，特别可设 $\mathfrak{B}$ 的 Z-基为 $\{1,\omega\}$，且可设 $\mathrm{Im}\,\omega>0$（这里当然要固定一个由 K 到 C 的嵌入）。于是

$$N(\mathfrak{B})=\frac{\omega-\bar{\omega}}{i\sqrt{|d|}}=\frac{2}{\sqrt{|d|}}\mathrm{Im}\,\omega,$$

$$N(m\omega+n)=m^2|\omega|^2+2mn\mathrm{Re}\,\omega+n^2,\ m,\ n\in Z,$$

$$\zeta_K(s\mid A)=\frac{|d|^{-\frac{s}{2}}}{w_K}\sum_{m,n\in Z}{}'(f(m,n))^{-s},\ \mathrm{Re}\,s>1, \tag{3.111}$$

（这里"′"表示 m、n 不能同时为零）其中

$$f(m,n)=\frac{|m\omega+n|^2}{2\,\mathrm{Im}\,\omega}$$

是一个判别式为 -1 的实系数的二元二次正定型。由此可得下面定理。

定理 2.1 (Kronecker) 对虚二次域 $K=Q(\sqrt{d})$，设理想类 A^{-1} 含有一个理想 [1] $Z\oplus\omega Z$，其中 $\mathrm{Im}\,\omega>0$，例如

$$A=\left[\left[a,\ \frac{b+\sqrt{d}}{2}\right]\right],\ |b|\leqslant a\leqslant\frac{b^2-d}{4a},$$

$$a,\ b\in Z,\ 4a\mid b^2-d,$$

时，可取 $\omega=\dfrac{-b+\sqrt{d}}{2a}$，则有

$$\zeta_K(s\mid A)=\frac{\rho_K}{s-1}+\xi_0(A)+O(|s-1|),\ \text{如}\ s\to1, \tag{3.112}$$

其中

$$\rho_K=\frac{2\pi}{w_K\sqrt{|d|}},\ w_K=|U_K|,$$

---

1) 可能是分式理想。

$$\xi_0(A)=\rho_{\mathbb{K}}(2\gamma-\log(2\sqrt{|d|}|\eta(\omega)|^4\operatorname{Im}\omega)),$$

γ 是 Euler 函数，$\eta(\omega)$ 是 Dedekind η-函数。

证明 见 C.L. Siegel《Advanced Analytic Number Theory》Tata Inst.

对实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$，它的单位群 $U_{\mathbb{K}}=\{\pm\varepsilon^n\,|\,n\in\mathbb{Z}\}$，其中 ε 为基本单位。于是由(3.109)有

$$\zeta_{\mathbb{K}}(s|A)=\frac{\mathbb{N}(\mathfrak{B})^s}{2}\sum_{\lambda\in\mathfrak{B}/\varepsilon}{}'\frac{1}{|\mathbb{N}(\lambda)|^s},\ \operatorname{Re}s>1,$$

$$\text{若 } \mathbb{K} \text{ 为实二次域。} \tag{3.113}$$

以 $\Delta=\mathbb{N}(\mathfrak{B})d^{\frac{1}{2}}$ 记 $\mathfrak{B}$ 的判别式，$\lambda'=\sigma(\lambda)$ 记 λ 在 $\operatorname{Gal}(\mathbb{K}/\mathbb{Q})$ 中的唯一的非恒等自同构 σ 下的象，由(3.113)可得

$$2d^{s/2}\zeta_{\mathbb{K}}(s|A)=\sum_{\lambda\in\mathfrak{B}/\varepsilon}{}'\frac{\Delta^s}{|\lambda\lambda'|^s}. \tag{3.114}$$

由(3.114)，并用一种现在称为“Hecke 技巧”的方法，可以证明下面的定理。

定理 2.2(Hecke) 对实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$，设理想类 A^{-1} 含有一个理想[1] $\mathbb{Z}+\omega\mathbb{Z}$，其中 $\omega>\omega'=\sigma(\omega)$，$\sigma$ 是 $\operatorname{Gal}(\mathbb{K}/\mathbb{Q})$ 中的唯一的非恒等自同构，即 $\operatorname{Gal}(\mathbb{K}/\mathbb{Q})=\langle\sigma\rangle$，例如

$$A=\left[\left[a,\ \frac{b+\sqrt{d}}{2}\right]\right],\ |b|\leqslant a\leqslant\frac{d-b^2}{4a},\ a,\ b\in\mathbb{Z},$$

$$4a\,|\,d-b^2$$

时，可取 $\omega=\dfrac{-b+\sqrt{d}}{2a}$，则有

$$\zeta_{\mathbb{K}}(s|A)=\frac{\rho_{\mathbb{K}}}{s-1}+\xi_0(A)+O(|s-1|),\ \text{如 } s\to1, \tag{3.115}$$

其中

$$\rho_{\mathbb{K}}=\frac{2\log\varepsilon}{\sqrt{d}},$$

$$\xi_0(A)=\rho_{\mathbb{K}}(2\gamma-\log\sqrt{d})+\frac{1}{\sqrt{d}}$$

---

1) 可能是分式理想。

$$\times\int_{-\log\varepsilon}^{\log\varepsilon}\left(\log\left(\frac{e^{v}+e^{-v}}{\omega-\omega'}\right)-\log\left|\eta\left(\frac{\omega+i\omega'e^{-v}}{1+ie^{-v}}\right)\right|^{4}\right)dv,$$

ε 是基本单位。

证明 见 Hecke 全集 pp.198—207.

2.2 二次域的一种 L-函数

对二次域 $K=Q(\sqrt{d})$ 的一个狭义理想类 A，和一个 mod k 的 Dirichlet 特征 χ，我们定义一种 L-函数如下：

$$\widetilde{L}(s,\ \chi|A)=\begin{cases}\dfrac{1}{w_K}\sum\limits_{\substack{\lambda\in\mathfrak{A}\\ \lambda\neq 0}}\dfrac{\chi(N(\lambda)/N(\mathfrak{A}))}{(N(\lambda)/N(\mathfrak{A}))^{s}}, & \text{如 } d<0,\ \mathrm{Re}\,s>1;\\ \dfrac{1}{w_K}\sum\limits_{\substack{\lambda\in\mathfrak{A}/\varepsilon_+\\ \lambda\gg 0}}\dfrac{\chi(N(\lambda)/N(\mathfrak{A}))}{(N(\lambda)/N(\mathfrak{A}))^{s}}, & \text{如 } d>0,\ \mathrm{Re}\,s>1\end{cases}\tag{3.116}$$

这里 $\mathfrak{A}$ 是 A 中的一个整理想；λ 跑过 $\mathfrak{A}$ 中的代数整数，并满足相应的条件；$\lambda\gg 0$ 指 $\lambda>0$ 且 $\lambda'=\sigma(\lambda)>0$，这时称 λ 为全正的；ε_+ 是全正基本单位，即对 $K=Q(\sqrt{d})\ (d>0)$ 的基本单位 ε，有

$$\varepsilon_+=\begin{cases}\varepsilon, & \text{如 } N(\varepsilon)=1;\\ \varepsilon^2, & \text{如 } N(\varepsilon)=-1,\end{cases}$$

最后 $w_K=1,\ 2,\ 4,\ 6$，视 $d>0,\ d<-4,\ d=-4,\ d=-3$ 而定。

(3.116) 右边的级数显然在 $\mathrm{Re}\ s\geqslant\sigma_0>1$（$\sigma_0$ 为任一个给定的大于 1 的正常数）时绝对且一致收敛、从而容易看出它与 A 中的整理想 $\mathfrak{A}$ 的选取无关，所以上述定义是合理的。并且 $\widetilde{L}(s,\ \chi|A)$ 是 $\mathrm{Re}\ s>1$ 中的一个解析函数。

再命

$$\widetilde{L}(s,\ \chi)=\sum_{A}\widetilde{L}(s,\ \chi|A),\ \mathrm{Re}\,s>1\tag{3.117}$$

其中 A 跑过 K 的狭义理想类群。易见 $\widetilde{L}(s,\ \chi)$ 是 $\mathrm{Re}\,s>1$ 中的一个解析函数。

本小节的目的在于证明下面的定理。

定理 2.3 对上述定义的 $\widetilde{L}(s,\ \chi)$，我们有

$$L(s,\ \chi)L(s,\ \chi\chi_d)=\widetilde{L}(s,\ \chi),\ \mathrm{Re}\,s>1,\tag{3.118}$$

这里 $L(s, \chi)$, $L(s, \chi\chi_d)$ 为通常的 Dirichlet 函数 L-函数, $\chi_d(*) = \left(\frac{d}{*}\right)$ 是 Kronecker 符号。

附注　可以由(3.118)把 $\widetilde{L}(s, \chi)$ 解析开拓到整个 s 平面，并且它只会在 $s=1$ 处方可能有一个一阶极点，同时它还会有函数方程，所以可以预料，对每一个类 A, $\widetilde{L}(s, \chi|A)$ 也会有相应的结论，这里由于与我们所关心的 Gauss 类数问题没有很大的联系，就不讨论了，但我们指出，在一些特殊情况下，我们(见参考文献[69])已证明了这一点。

定理的证明　设 $\operatorname{Re} s>1$, 则我们有

$$L(s, \chi)L(s, \chi\chi_d) = \sum^{\infty} \frac{\chi(n)}{n^s} \sum_{m=1}^{\infty} \frac{\chi(m)\chi_d(m)}{m^s}$$

$$= \sum^{\infty} \frac{\chi(n)}{n^s} \sum_{1\leq m|n} \chi_d(m),$$

所以由第二章§1.7的引理1.28，即有

$$w_K L(s, \chi)\, L(s, \chi\chi_d) = \sum^{\infty} \frac{\chi(n)}{n^s} \psi_0(n)$$

$$= \sum_{j=1}^{H} \sum_{\substack{x, y\in \mathbf{Z} \\ F_j(x,y)>0 \\ (x,y)\text{为原解}}} \chi(F_j(x, y))F_j(x, y)^{-s}, \tag{3.119}$$

这里 $F_j(x, y) = a_jx^2 + b_jxy + c_jy^2$ 跑过判别式为 d 的二元二次原型类群的完全代表元组($d<0$ 时，只考虑正定型)，并可以要求 $a_j>0$。

对一个固定的判别式为 d 的二元二次原型 $F_j(x, y) = a_jx^2 + b_jxy + c_jy^2$, 当 (x, y) 为原解时，命

$$\lambda = a_jx + \frac{b_j - \sqrt{d}}{2}y,$$

则有 $F_j(x, y) = \frac{1}{a_j}\lambda\lambda' = \frac{1}{a_j}\lambda\sigma(\lambda) = \frac{1}{a_j}N(\lambda)$。注意到 $a_j>0$, 即知 F_j 所对应的整理想为

$$\mathfrak{A}_j = \left[a_j, \frac{-b_j+\sqrt{d}}{2}\right] = a_j\mathbf{Z} \oplus \frac{-b_j+\sqrt{d}}{2}\mathbf{Z},$$

$$N(\mathfrak{A}_j) = a_j,$$

并有 $\lambda\in\mathfrak{A}_j$。

根据原解的定义，在 $d<0$ 时，$F_j(x, y)>0$ 且 (x, y) 为原解，等价于 $\lambda\neq 0$；而在 $d>0$ 时，$F_j(x, y)>0$ 且 (x, y) 为原解，等价于 $\lambda\gg 0$，且 $1\leqslant\frac{\lambda}{\lambda'}<\varepsilon_+^2$。这样由(3.119)即有

$$
\begin{aligned}
& w_K L(s, \chi)L(s, \chi\chi_d) \\
&= \begin{cases} \sum\limits_{j=1}^{H}\sum\limits_{\substack{\lambda\in\mathfrak{A}_j\\ \lambda\neq 0}} \dfrac{\chi(N(\lambda)/N(\mathfrak{A}_j))}{(N(\lambda)/N(\mathfrak{A}_j))^s}, & \text{如 } d<0; \\ \sum\limits_{j=1}^{H}\sum\limits_{\substack{\lambda\in\mathfrak{A}_j/\varepsilon_+\\ \lambda\gg 0}} \dfrac{\chi(N(\lambda)/N(\mathfrak{A}_j))}{(N(\lambda)/N(\mathfrak{A}_j))^s}, & \text{如 } d>0 \end{cases} \\
&= w_K\tilde{L}(s, x),
\end{aligned}
$$

最后一步用了 $\tilde{L}(s, \chi)$ 的定义(3.116)。定理证毕。

2.3 $\tilde{L}(s, \chi|A)$ 的极限公式($d<0$ 时)

当 $d<0$ 时，由上小节定理 3.6 的证明可见

$$
w_K\tilde{L}(s, \chi|A)=\sum_{\substack{m,n=-\infty\\ (m,n)\neq(0,0)}}^{+\infty}\chi(F(m,n))(F(m,n))^{-s}, \mathrm{Re}\, s>1. \tag{3.120}
$$

其中 $F(x, y)=ax^2+bxy+cy^2$ 是 $A\left(\ni\left[a, \dfrac{-b+\sqrt{d}}{2}\right]\right)$ 所对应的判别式为 d 的二元二次原型，且可设

$$
|b|\leqslant a\leqslant c,\ d=b^2-4ac,\ a,\ b,\ c\in\boldsymbol{Z},\ g.c.d.(a,\ b,\ c)=1. \tag{3.121}
$$

(3.120)的右边是

$$
L\overset{\mathrm{def}}{=\!=}\sum_{\substack{-\infty<m,n<+\infty\\ (m,n)\neq(0,0)}}\frac{\chi(am^2+bmn+cn^2)}{(am^2+bmn+cn^2)^s}, \mathrm{Re}\, s>1,
$$

其中 χ 是 mod k 的 Dirichlet 特征。我们有

$$
\begin{aligned}
L &= 2\sum_{m=1}^{\infty}\frac{\chi(am^2)}{(am^2)^s}+2\sum_{n=1}^{\infty}\sum_{m=-\infty}^{+\infty}\frac{\chi(am^2+bmn+cn^2)}{(am^2+bmn+cn^2)^s} \\
&= 2\chi(a)a^{-s}L(2s, \chi^2)+2\sum_{n=1}^{\infty}E_n, \mathrm{Re}\, s>1,
\end{aligned} \tag{3.122}
$$

这里

$$E_n=\sum_{m=-\infty}^{+\infty}\frac{\chi(am^2+bmn+cn^2)}{(am^2+bmn+cn^2)^s},\ n\geqslant 1,\ \mathrm{Re}\,s>1. \tag{3.123}$$

对任一个实数 x，命

$$E_n(x)=\sum_{m=-\infty}^{+\infty}\frac{\chi(am^2+bmn+cn^2)}{(a(m+nx)^2+b(m+nx)n+cn^2)^s},$$
$$n\geqslant 1,\ \mathrm{Re}\,s>1. \tag{3.124}$$

则有 $E_n=E_n(0)$，并且 $E_n(x)$是 x 的周期为 k 的周期函数，故

$$E_n(x)=\sum_{u=-\infty}^{+\infty}a_u e^{2\pi iux/k}, \tag{3.125}$$

这里

$$\begin{aligned}a_u&=\frac{1}{k}\int_0^k E_n(x)e^{-2\pi iux/k}dx\\&=\frac{1}{k}\sum_{m=-\infty}^{+\infty}\int_0^k\frac{\chi(am^2+bmn+cn^2)}{(a(m+nx)^2+b(m+nx)n+cn^2)^s}e^{-2\pi iux/k}dx,\end{aligned} \tag{3.126}$$

这里与以上的有关收敛、绝对收敛、一致收敛，以及和号与积分号的交换等等的要求，在 s 满足 $\mathrm{Re}\,s\geqslant\sigma_0>1$($\sigma_0$ 为任一给定的大于1的正常数)下，显然都满足，以下不再赘述了。令 $m\mapsto m+m_1kn$，即由(3.126)可得

$$\begin{aligned}a_u&=\frac{1}{k}\sum_{m(\mathrm{mod}\,kn)}\chi(am^2+bmn+cn^2)\\&\quad\times\sum_{m_1=-\infty}^{+\infty}\int_0^k\frac{e^{-2\pi iux/k}dx}{F(m+n(x+km_1),\ n)^s}\\&=\frac{1}{k}\sum_{m(\mathrm{mod}\,kn)}\chi(am^2+bmn+cn^2)\int_{-\infty}^{+\infty}\frac{e^{-2\pi iux/k}}{F(m+nx,\ n)^s}dx,\end{aligned}$$

再令 $m+nx\mapsto nx$，即有

$$\begin{aligned}a_u&=\frac{n^{-2s}}{k}\sum_{m(\mathrm{mod}\,kn)}\chi(F(m,\ n))e^{2\pi ium/(kn)}\\&\quad\times\int_{-\infty}^{+\infty}\frac{e^{-2\pi iux/k}}{F(x,\ 1)^s}dx,\end{aligned} \tag{3.127}$$

易见有

$$\sum_{m(\bmod kn)}\chi(F(m,n))e^{2\pi ium/(kn)}$$

$$=\begin{cases} n\sum\limits_{m(\bmod k)}\chi(F(m,n))e^{2\pi ium/(kn)}, & \text{如 } n\mid u; \\ 0, & \text{否则}, \end{cases}$$

由此及(3.127)即有

$$a_u=\begin{cases} \dfrac{n^{1-2s}}{k}I(s,u)\sum\limits_{m(\bmod k)}\chi(F(m,n))e^{2\pi ium/(kn)}, & \text{如 } n\mid u; \\ 0, & \text{否则}. \end{cases} \tag{3.128}$$

这里

$$I(s,u)=\int_{-\infty}^{+\infty}\frac{e^{-2\pi iux/k}}{(ax^2+bx+c)^s}dx,\ \operatorname{Re} s\geqslant 1, u\in \mathbb{Z}.$$

命 $$x\longrightarrow \frac{\sqrt{|d|}}{2a}x-\frac{b}{2a},\ \text{即得}$$

$$I(s,u)=|d|^{\frac{1}{2}-s}a^{s-1}2^{2s-1}e^{\pi ibu/(ak)}$$
$$\times\int_{-\infty}^{+\infty}\frac{e^{-2\pi iu\sqrt{|d|}x/(2ak)}}{(x^2+1)^s}dx,$$

再计及(参见[20]p.959的公式5)

$$\int_{-\infty}^{+\infty}\frac{e^{-2\pi ixY}}{(x^2+1)^s}dx$$

$$=\begin{cases} \dfrac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)}, & \text{如 } Y=0, \operatorname{Re} s>\dfrac{1}{2}; \\ \dfrac{2\Gamma\left(\frac{1}{2}\right)}{\Gamma(s)}(\pi|Y|)^{s-\frac{1}{2}}K_{s-\frac{1}{2}}(2\pi|Y|), & \\ & \text{如 } Y\neq 0,\ Y\in R,\ \operatorname{Re} s>0 \end{cases} \tag{3.129}$$

(这里 $\Gamma(*)$ 是 Γ 函数, K_ν 为 Bessel 函数), 即有

$$I(s,o)=|d|^{\frac{1}{2}-s}a^{s-1}2^{2s-1}\frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)},\ \operatorname{Re} s>\frac{1}{2},$$

$$I(s,\ u)=\frac{(2\pi)^s}{\Gamma(s)}\sqrt{\frac{2}{a}}\,k^{\frac{1}{2}-s}\,|d|^{\frac{1}{4}-\frac{s}{2}}|u|^{s-\frac{1}{2}}$$

$$\times K_{s-\frac{1}{2}}\left(\frac{\pi|u|\sqrt{|d|}}{ak}\right)e^{\pi ibu/(ak)},\ \text{如}\ u\neq 0,\ \operatorname{Re} s>0.$$

于是由(3.128)即得,在$\operatorname{Re} s>\frac{1}{2}$时,有

$$a_0=\frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(s-\frac{1}{2}\right)}{k\Gamma(s)}|d|^{\frac{1}{2}-s}a^{s-1}2^{2s-1}n^{1-2s}$$

$$\times\sum_{m(\bmod k)}\chi(F(m,\ n));$$

$$a_u=0,\ \text{如}\ n\nmid u;$$

$$a_u=\frac{(2\pi)^s}{\Gamma(s)k^s}\sqrt{\frac{2}{ak}}|u|^{s-\frac{1}{2}}|d|^{\frac{1}{4}-\frac{s}{2}}n^{1-2s}$$

$$\times K_{s-\frac{1}{2}}\left(\frac{\pi|u|\sqrt{|d|}}{ak}\right)e^{\pi ibu/(ak)}.$$

$$\sum_{m(\bmod k)}\chi(F(m,\ n))e^{2\pi ium/(kn)},\ \text{如}\ n\mid u,\ \text{但}\ u\neq 0,$$

以此代入$E_n(x)$的展开式(3.125),再令$x=0$,即得,在$\operatorname{Re}s>1$时,有

$$E_n=E_n(0)=\sum_{u=-\infty}^{+\infty}a_u$$

$$=\frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)k}|d|^{\frac{1}{2}-s}a^{s-1}2^{2s-1}n^{1-2s}\sum_{m(\bmod k)}\chi(F(m,\ n))$$

$$+\frac{2^{s+\frac{3}{2}}\pi^s n^{\frac{1}{2}-s}}{\Gamma(s)k^s\sqrt{ak}}|d|^{\frac{1}{4}-\frac{s}{2}}\sum_{u=1}^{\infty}u^{s-\frac{1}{2}}K_{s-\frac{1}{2}}\left(\frac{\pi un\sqrt{|d|}}{ak}\right)$$

$$\times\sum_{m(\bmod k)}\chi(F(m,\ n))\cos\frac{2\pi un}{k}\left(\frac{m}{n}+\frac{b}{2a}\right),$$

再以此代入(3.122)即得,在$\operatorname{Re} s>1$时,有

$$L=\frac{2\chi(a)}{a^s}L(2s,\ \chi^2)$$

$$+\frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)k}|d|^{\frac{1}{2}-s}a^{s-1}4^s\sum_{}^{\infty}n^{1-2s}\sum_{m(\bmod k)}\chi(F(m,n))$$

$$+\frac{2^{s+\frac{5}{2}}\pi^s}{\Gamma(s)\sqrt{a}kk^s}|d|^{\frac{1}{4}-\frac{s}{2}}\sum_{u,n=1}^{\infty}n^{\frac{1}{2}-s}u^{s-\frac{1}{2}}K_{s-\frac{1}{2}}\left(\frac{\pi un\sqrt{|d|}}{ak}\right)$$

$$\cdot\sum_{m(\bmod k)}\chi(F(m,n))\cos\frac{2\pi un}{k}\left(\frac{m}{n}+\frac{b}{2a}\right)$$

$$=\frac{2\chi(a)}{a^s}L(2s,\chi^2)+\frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)k}|d|^{\frac{1}{2}-s}a^{s-1}4^s$$

$$\cdot\sum_{n=1}^{\infty}n^{1-2s}\sum_{m(\bmod k)}\chi(F(m,n))+\frac{2^{s+\frac{5}{2}}\pi^s}{\Gamma(s)\sqrt{a}kk^s}|d|^{\frac{1}{4}-\frac{s}{2}}$$

$$\cdot\sum_{u=1}^{\infty}u^{s-\frac{1}{2}}K_{s-\frac{1}{2}}\left(\frac{\pi u\sqrt{|d|}}{ak}\right)\sum_{1\leqslant n|u}n^{1-2s}$$

$$\cdot\sum_{m(\bmod k)}\chi(F(m,n))\cos\frac{2\pi u}{k}\left(\frac{m}{n}+\frac{b}{2a}\right),$$

这样，由(3.120)即有

$$\tilde{L}(s,\chi|A)=\frac{2\chi(a)}{a^s w_K}L(2s,\chi^2)$$

$$+\frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)kw_K}|d|^{\frac{1}{2}-s}a^{s-1}4^s\sum^{\infty}n^{1-2s}\sum_{m(\bmod k)}\chi(F(m,n))$$

$$+\frac{2^{s+\frac{5}{2}}\pi^s|d|^{\frac{1}{4}-\frac{s}{2}}}{w_K\Gamma(s)\sqrt{a}kk^s}\sum_{u=1}^{\infty}u^{s-\frac{1}{2}}K_{s-\frac{1}{2}}\left(\frac{\pi u\sqrt{|d|}}{ak}\right)$$

$$\cdot\sum_{1\leqslant n|u}n^{1-2s}\sum_{m(\bmod k)}\chi(F(m,n))\cos\frac{2\pi u}{k}\left(\frac{m}{n}+\frac{b}{2a}\right),$$

$$\operatorname{Re}s>1, \tag{3.130}$$

当 $0<\sigma_0\leqslant\operatorname{Re}s\leqslant 2$ 时(其中 σ_0 为一个给定的小于 2 而大于 0 的正常数)，则由参考文献[20]p.959 的公式 8 有

$$K_{s-\frac{1}{2}}\left(\frac{\pi u\sqrt{|d|}}{ak}\right)$$

$$=\frac{\sqrt{\frac{\pi}{2}}}{\Gamma(s)}\left(\frac{\pi u\sqrt{|d|}}{ak}\right)^{s-\frac{1}{2}}e^{-\pi u\sqrt{|d|}/(ak)}$$

$$\cdot\int_0^{\infty}e^{-\pi u\sqrt{|d|}v/(ak)}v^{s-1}\left(1+\frac{v}{2}\right)^{s-1}dv,$$

$$\ll u^{\sigma_0-\frac{1}{2}}e^{-\pi\sqrt{|d|}u/(ak)}|\Gamma(s)|^{-1},$$

这里“≪”所含的正常数仅与 σ_0, $|d|$, k, F 有关,而与 u 无关。由此可知(3.130)的第三项

$$\ll|\Gamma(s)|^{-2}\sum_{u=1}^{\infty}e^{-\pi\sqrt{|d|}u/(ak)}\sum_{1\leqslant n|u}n^{2\sigma_0-1}$$
$$\ll|\Gamma(s)|^{-2},\quad \sigma_0\leqslant \operatorname{Re} s\leqslant 2,$$

这里“≪”所含的正常数仅与 σ_0, $|d|$, k, F 有关。因此(3.130)的第三项在 $\operatorname{Re} s>0$ 时是解析的。

又对(3.130)的第二项所涉及的级数,用§1.3的 Hurwitz ζ-函数即知,在 $\operatorname{Re} s>1$, 且 $s\to1$ 时,有

$$\begin{aligned}&\sum_{n=1}^{\infty}n^{1-2s}\sum_{m(\bmod k)}\chi(F(m,n))\\
&=\sum_{1\leqslant m,n\leqslant k}\chi(F(m,n))k^{1-2s}\zeta\left(2s-1,\frac{n}{k}\right)\\
&=\sum_{1\leqslant m,n\leqslant k}\chi(F(m,n))\left(\frac{1}{k}-\frac{2\log k}{k}(s-1)+O(|s-1|^2)\right)\\
&\quad\times\left(\frac{1}{2(s-1)}-\psi\left(\frac{n}{k}\right)+O(|s-1|)\right)\\
&=\frac{1}{2k(s-1)}\sum_{m,n(\bmod k)}\chi(F(m,n))\\
&\quad-\frac{\log k}{k}\sum_{m,n(\bmod k)}\chi(F(m,n))\\
&\quad-\frac{1}{k}\sum_{1\leqslant m,n\leqslant k}\chi(F(m,n))\psi\left(\frac{n}{k}\right)+O(|s-1|),\quad s\to1.\end{aligned}$$

因此(3.130)的第二项是 s 的一个半纯函数,当 $\operatorname{Re} s>\frac{1}{2}$ 时,仅可能在 $s=1$ 处有一阶极点外,均是解析的,并在 $s=1$ 处有 Laurent 展开式或 Taylor 展开式(视 $s=1$ 为其极点与否)。

由上述的推导,由(3.130)可知,我们已得到了$\tilde{Z}(s,\chi|A)$在 $\operatorname{Re} s>\frac{1}{2}$ 时的解析开拓,它在 $\operatorname{Re} s>\frac{1}{2}$ 时,仅可能在 $s=1$ 处有一个一阶极点,并在 $s=1$ 处有展开式

$$\widetilde{L}(s,\ \chi|A)=\frac{1}{s-1}\ \frac{2\pi}{w_K k^2\sqrt{|d|}}$$
$$\cdot\sum_{m,n(\mathrm{mod}\,k)}\chi(F(m,\ n))+\frac{2\chi(a)}{w_K a}L(2,\ \chi^2)$$
$$-\frac{4\pi}{w_K k^2\sqrt{|d|}}\log\left(k\sqrt{\frac{|d|}{a}}\right)\sum_{m,n(\mathrm{mod}\,k)}\chi(F(m,\ n))$$
$$-\frac{4\pi}{w_K k^2\sqrt{|d|}}\sum_{1\leqslant m,n\leqslant k}\chi(F(m,\ n))\psi\left(\frac{n}{k}\right)$$
$$+\frac{8\pi}{w_K k\sqrt{|d|}}\sum_{u=1}^{\infty}e^{2\pi iu\sqrt{d}/(2ak)}\sum_{1\leqslant n|u}n^{-1}$$
$$\cdot\sum_{m(\mathrm{mod}\,k)}\chi(F(m,\ n))\cos\frac{2\pi u}{k}\left(\frac{m}{n}+\frac{b}{2a}\right)$$
$$+O(|s-1|),\ s\to 1. \tag{3.131}$$

其中与往常一样，$w_K=|U_K|$，以上推导中用到

$$K_{\frac{1}{2}}(z)=\sqrt{\frac{\pi}{2z}}e^{-z},\ 如\ z>0, \tag{3.132}$$

与

$$\frac{\Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{1}{2}-s\right)}{\Gamma(s)k}|d|^{\frac{1}{2}-s}a^{s-1}4^s$$
$$=\frac{4\pi}{k\sqrt{|d|}}-\frac{4\pi}{k\sqrt{|d|}}\log\frac{|d|}{a}$$
$$\cdot(s-1)+O(|s-1|^2),\ s\to 1.$$

附注 为得到 $\widetilde{L}(s,\ \chi|A)$ 在 $\mathrm{Re}\,s>0$ 时的奇点的信息，我们再分析一下(3.130)。由上述推导可知，除 $s=1$ 以外，可能的奇点，仅可能由第一、二项产生。第一项仅可能在 $s=\frac{1}{2}$ 处有一个一阶极点，这是当 χ^2 为主特征，即 χ 为实特征时出现。第二项也仅可能在 $s=\frac{1}{2}$ 处有一个一阶极点，它由 $\Gamma\left(s-\frac{1}{2}\right)$ 产生，但是第二项所涉及的级数在 $s=\frac{1}{2}$ 处有值

$$\sum_{1\leqslant m,n\leqslant k}\chi(F(m,\ n))\zeta\left(0,\ \frac{n}{k}\right)$$

$$=\sum_{1\leqslant m,n\leqslant k}\chi(F(m,\ n))\left(\frac{1}{2}-\frac{n}{k}\right). \tag{3.133}$$

因此当(3.133)右边的值为零时，第二项在 $s=\frac{1}{2}$ 处是解析的。所以讨论(3.133)右边的和是很有兴趣的。很可能是

$$\sum_{1\leqslant m,n\leqslant k}\chi(F(m,\ n))\left(\frac{1}{2}-\frac{n}{k}\right)$$

$$=\begin{cases}0, & \text{如 } \chi \text{ 不是 } \bmod k \text{ 实特征；}\\ -\dfrac{\chi(a)}{2}\varphi(k), & \text{如 } \chi \text{ 是 } \bmod k \text{ 实特征。}\end{cases}$$

留给读者来探讨。

以下来讨论(3.131)的几个特例。

首先取 $k=1$，则有

$$\tilde{L}(s,\ \chi_0|A)$$

$$=\frac{\rho_K}{s-1}+\rho_K\left(2\gamma+\frac{b\pi i}{6a}-2\log\sqrt{\frac{|d|}{a}}-4\log\eta(\omega_A)\right)$$

$$+O(|s-1|),\quad s\to 1. \tag{3.134}$$

其中

$$\rho_K=\frac{2\pi}{w_K\sqrt{|d|}},\quad \omega_A=\frac{b+\sqrt{d}}{2a}.$$

我们不详述(3.134)的详细证明了，读者不难用本章的知识完成它的证明。

又有

$$L(s,\ \chi_0)L(s,\ \chi_d)=\frac{L(1,\ \chi_d)}{s-1}+\gamma L(1,\ \chi_d)$$

$$+L'(1,\ \chi_d)+O(|s-1|),\quad s\to 1, \tag{3.135}$$

由(3.134)与(3.135)即得

$$L(1,\ \chi_d)=h_K\rho_K, \tag{3.136}$$

$$L'(1,\ \chi_d)=h_K\rho_K\gamma+\rho_K$$

$$\cdot\sum_{A=\left[\left[a,\frac{-b+\sqrt{d}}{2}\right]\right]}\left(\frac{6\pi i}{6a}-2\log\sqrt{\frac{|d|}{a}}-4\log\eta(\omega_A)\right), \tag{3.137}$$

这里 h_K 是 $\mathbb{K}$ 的类数，

$$A=\left[\left[a,\ \frac{-b+\sqrt{d}}{2}\right]\right]$$

跑过 $\mathscr{C}_0(d)$（K 的理想类群）。

(3.136) 与已知的结果完全吻合。特别地，当 $h_K=1$ 时，由 (3.137) 可得

$$L'(1,\ \chi_d)=\rho_K\left(\gamma+\frac{b_0\pi i}{6}-\log|d|-4\log\eta\left(\frac{b_0+\sqrt{d}}{2}\right)\right),$$

$$\text{如 } h_K=1,\ d<0, \tag{3.138}$$

这里 $b_0=1$ 或 0，视 d 为奇或偶而定。

再取 $A=\left[\left[1,\ \frac{-b_0+\sqrt{d}}{2}\right]\right]$，$b_0$ 如上所述。再取正基本判别式 k，使得 $g.c.d.(k,\ d)=1$，且 k 至少有两个不同的素因子。令 χ 为 mod k 的 Kronecker 符号。则由 (3.131)、定理 1.3 以及第二章 §1.6 的定理 1.8，即得

$$\widetilde{L}(1,\ \chi|A)=\frac{\pi^2}{3w_K}\prod_{p|k}(1-p^{-2})$$

$$+\frac{4\rho_K}{k}\sum_{u=1}^{\infty}e^{2\pi iu\sqrt{d}/(2k)}\sum_{1\leqslant n|u}n^{-1}$$

$$\cdot\sum_{m(\mathrm{mod}\ k)}\chi\left(m^2+b_0mn+\frac{b_0-d}{4}n^2\right)\cos\frac{2\pi u}{k}\left(\frac{m}{n}+\frac{b_0}{2}\right),$$

注意后一个和的绝对值

$$\leqslant k\sum_{u=1}^{\infty}ue^{-\frac{\pi\sqrt{|d|}}{k}u}=\frac{ke^{-\frac{\pi}{k}\sqrt{|d|}}}{(1-e^{-\frac{\pi}{k}\sqrt{|d|}})^2},$$

于是得到下面的引理。

引理 2.1 设 d 为一个负的基本判别式，k 为另一个正的基本判别式，k 至少有两个不同的素因子，χ 为 mod k 的 Kronecker 符号，

$$A=\left[\left[1,\ \frac{b_0+\sqrt{d}}{2}\right]\right],$$

其中 $b_0=0$ 或 1，视 d 为偶或奇而定，则有

$$\left|\tilde{Z}(1, \chi|A) - \frac{\pi^2}{3w_K}\prod_{p|k}(1-p^{-2})\right| \leqslant \frac{4\rho_K e^{-\pi\sqrt{|d|}/k}}{(1-e^{-\pi\sqrt{|d|}/k})^2},$$

其中 w_K 为 $K=Q(\sqrt{d})$ 的单位根群的阶,

$$\rho_K = \frac{2\pi}{w_K\sqrt{|d|}}.$$

2.4 $\tilde{Z}(s, \chi|A)$ 的极限公式($d>0$ 时)

设 $d>0$ 为一个给定的正的基本判别式，有理整数 a, b, c 满足

$$g.c.d.(a, b, c)=1, \ d=b^2-4ac, \ a>0.$$

考虑 $K=Q(\sqrt{d})$ 的整理想 $\mathfrak{A}=\left[a, \frac{-b+\sqrt{d}}{2}\right]$ 所属的狭义理想类 A。整理想 $\mathfrak{A}^*=\sqrt{d}\,\mathfrak{A}$ 与 $\mathfrak{A}$ 属于同一个广类。命

$$\alpha=\frac{b+\sqrt{d}}{2a}, \quad \alpha'=\frac{b-\sqrt{d}}{2a}. \tag{3.139}$$

现在考虑复平面 Z 到复平面 z 的分式线性变换

$$z=\frac{Z-\alpha}{Z-\alpha'} \ (z=x+iy, \ Z=X+iY),$$

它的逆变换是

$$Z=\frac{\alpha' z-\alpha}{z-1}.$$

Z 与 z 之间的变换情况可列表如下:

Z	α'	0	$\frac{b}{2a}=\frac{\alpha+\alpha'}{2}$	α	∞	Γ	Z_0^*	Z_0
z	∞	$\frac{\alpha}{\alpha'}$	-1	0	1	$iy,\ y>0$	$i\varepsilon_+^{-2}$	$i\varepsilon_+^2$

这里 Γ 是 Z 平面上以 $\frac{\alpha+\alpha'}{2}=\frac{b}{2a}$ 为圆心, $\frac{\alpha-\alpha'}{2}=\frac{\sqrt{d}}{2a}$ 为半径, α 与 α' 为两个端点的上半圆周; ε_+ 是 $K=Q(\sqrt{d})$ 的全正基本单位, 而

$$Z_0=\frac{\alpha' i\varepsilon_+^2-\alpha}{i\varepsilon_+^2-1}=\alpha'+\frac{\sqrt{d}}{2a}\cdot\frac{2(\varepsilon_+^{-2}+i)}{\varepsilon_+^2+\varepsilon_+^{-2}}, \tag{3.140}$$

$$Z_0^* = \frac{\alpha' i\varepsilon_+^{-2} - \alpha}{i\varepsilon_+^{-2} - 1} = \alpha - \frac{\sqrt{d}}{2a} \cdot \frac{2(\varepsilon_+^{-2} - i)}{\varepsilon_+^2 + \varepsilon_+^{-2}}. \tag{3.141}$$

命

$$X_0 = \alpha' + \frac{\sqrt{d}}{2a} \cdot \frac{2\varepsilon_+^{-2}}{\varepsilon_+^2 + \varepsilon_+^{-2}}, \quad X_0^* = \alpha - \frac{\sqrt{d}}{2a} \cdot \frac{2\varepsilon_+^{-2}}{\varepsilon_+^2 + \varepsilon_+^{-2}}, \tag{3.142}$$

$$Y_0 = Y_0^* = \frac{\sqrt{d}}{2a} \frac{2}{\varepsilon_+^2 + \varepsilon_+^{-2}}, \tag{3.143}$$

则有

$$Z_0 = X_0 + iY_0, \ Z_0^* = X_0^* + iY_0^*,$$

Z_0, Z_0^* 均在上半圆周 Γ 上, 并有

$$\frac{1}{2}(X_0^* + X_0) = \frac{\alpha + \alpha'}{2} = \frac{b}{2a},$$

$$\frac{1}{2}(X_0^* - X_0) = \frac{\sqrt{d}}{2a} \cdot \frac{\varepsilon_+^2 - \varepsilon_+^{-2}}{\varepsilon_+^2 + \varepsilon_+^{-2}}.$$

设 k 为一个正整数, χ 为 mod k 的 Dirichlet 特征。

对满足 $\operatorname{Re} s = \sigma > 1$ 的复数 $s = \sigma + it$, 考虑以下的 Eisenstein 级数

$$E(s, Z, \mathfrak{A}) = \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{+\infty} \frac{\chi(am^2 + bmn + cn^2) Y^s}{|m + nZ|^{2s}},$$

$$\operatorname{Re} s > 1, \tag{3.144}$$

这里 $Z = X + iY$ 属于上半平面。右边的级数在 $\operatorname{Re} s \geqslant \sigma_0 > 1$ 是绝对且一致收敛的, 只要 σ_0 是一个给定的大于 1 的常数。因此 $E(s, Z, \mathfrak{A})$ 是 $\operatorname{Re} s > 1$ 中的解析函数。以下对所需要的收敛性不一一验证了。

对 Z 求偏微商可得

$$\frac{\partial E(s, Z, \mathfrak{A})}{\partial Z} = \frac{s}{2i} \sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{+\infty} \frac{\chi(am^2 + bmn + cn^2) Y^{s-1}}{(m + nZ)^{s+1}(m + n\bar{Z})^{s-1}},$$

$$\operatorname{Re} s > 1, \tag{3.145}$$

把它沿 Γ 的 Z_0 到 Z_0^* 这段圆弧(记为 $\Gamma(Z_0, Z_0^*)$)积分, 即令

$$I(s,\ \mathfrak{A})=\int_{\Gamma(Z_0,Z_0^*)}\frac{\partial E(s,\ Z,\ \mathfrak{A})}{\partial Z}dZ,\ \mathrm{Re}\,s>1. \qquad (3.146)$$

对 $Z\in\Gamma$，有

$$m+nZ=m+n\frac{\alpha' iy-\alpha}{iy-1}=\frac{iy\lambda'-\lambda}{iy-1},\ m,\ n\in\mathbb{Z},$$

其中

$$\lambda=m+n\alpha,\ \lambda'=m+n\alpha',\ m,\ n\in\mathbb{Z}.$$

又对 $Z=X+iY\in\Gamma$，有

$$Y=\frac{\sqrt{d}}{a}\cdot\frac{y}{y^2+1},\ dZ=\frac{\sqrt{d}}{a}\cdot\frac{i}{(iy-1)^2}dy.$$

因此有

$$\frac{Y^{s-1}dZ}{(m+nZ)^{s+1}(m+n\bar{Z})^{s-1}}=\frac{Y^{s-1}(m+n\bar{Z})^2}{|m+nZ|^{2(s+1)}}dZ$$

$$=i\left(\frac{\sqrt{d}}{a}\right)^s\frac{\lambda^2-\lambda'^2y^2+2iy\lambda\lambda'}{(y\lambda'^2+y^{-1}\lambda^2)^{s+1}}\cdot\frac{dy}{y^2},$$

以此代入(3.145)，即知，对 $Z\in\Gamma$，有

$$\frac{\partial E(s,\ Z,\ \mathfrak{A})}{\partial Z}=\frac{s}{2}\left(\frac{\sqrt{d}}{a}\right)^s$$

$$\cdot\sum_{\lambda\in[1,\alpha]}{}'\frac{(\lambda^2-\lambda'^2y^2+2iy\lambda\lambda')\chi(a\lambda\lambda')}{(y\lambda'^2+y^{-1}\lambda^2)^{s+1}}\cdot\frac{dy}{y^2},$$

这里求和号上的"′"表示 $\lambda\neq0$；$\lambda\in[1,\ \alpha]$ 表示 $\lambda=m+n\alpha,\ m,\ n\in\mathbb{Z},\ \lambda'=m+n\alpha'$。

因此在变量替换后，(3.146)成为

$$I(s,\ \mathfrak{A})=\frac{s}{2}\left(\frac{\sqrt{d}}{a}\right)^s$$

$$\times\int_{\varepsilon_+^2}^{\varepsilon_+^{-2}}\sum_{\lambda\in[1,\alpha]}{}'\frac{(\lambda^2-\lambda'y^2+2iy\lambda\lambda')\chi(a\lambda\lambda')}{(y\lambda'^2+y^{-1}\lambda^2)^{s+1}}\cdot\frac{dy}{y^2},\ \mathrm{Re}\,s>1,$$

令 $y\mapsto y^{-2}$，则有

$$I(s,\ \mathfrak{A})=-s\left(\frac{\sqrt{d}}{a}\right)^s$$

$$\times\int_{\varepsilon_+^{-1}}^{\varepsilon_+^{-2}}\sum_{\lambda\in[1,\alpha]}{}'\frac{(\lambda^2y^2-\lambda'^2y^{-2}+2i\lambda\lambda')\chi(a\lambda\lambda')}{(\lambda^2y^2+\lambda'^2y^{-2})^{s+1}}\cdot\frac{dy}{y}$$

$$= -2s\left(\frac{\sqrt{d}}{a}\right)^s$$

$$\times\int_0^\infty \sum_{\lambda\in[1,\alpha]/\varepsilon_+}' \frac{(\lambda^2y^2-\lambda'^2y^{-2}+2i\lambda\lambda')\chi(a\lambda\lambda')}{(\lambda^2y^2+\lambda'^2y^{-2})^{s+1}}\frac{dy}{y}$$

$$= -2s\left(\frac{\sqrt{d}}{a}\right)^s \sum_{\lambda\in[1,\alpha]/\varepsilon_+}' \chi(a\lambda\lambda')$$

$$\times\left(\int_0^\infty \frac{\lambda^2y^2-\lambda'^2y^{-2}}{(\lambda^2y^2+\lambda'^2y^{-2})^{s+1}}\frac{dy}{y}\right.$$

$$\left.+2i\lambda\lambda'\int_0^\infty\frac{dy}{y(\lambda^2y^2+\lambda'^2y^{-2})^{s+1}}\right),\ \mathrm{Re}\, s>1. \tag{3.147}$$

在 (3.147) 右边的第一个积分中，令 $y\mapsto\left|\frac{\lambda'}{\lambda}\right|y^{-1}$，即知其值改变了一个符号，所以是零；而在第二个积分中，令 $y\mapsto\left|\frac{\lambda'}{\lambda}\right|^{\frac{1}{2}}y$，即知其值为

$$\frac{1}{|\lambda\lambda'|^{s+1}}\int_0^\infty\frac{dy}{y(y^2+y^{-2})^{s+1}} = \frac{1}{|\lambda\lambda'|^{s+1}}\cdot\frac{\Gamma\left(\frac{s+1}{2}\right)^2}{4\Gamma(s+1)},$$

所以(3.147)成为

$$I(s,\ \mathfrak{A}) = -is\left(\frac{\sqrt{d}}{a}\right)^s\frac{\Gamma\left(\frac{s+1}{2}\right)^2}{\Gamma(s+1)}$$

$$\cdot\sum_{\lambda\in[1,\alpha]/\varepsilon_+}'\frac{\chi(a\lambda\lambda')\lambda\lambda'}{|\lambda\lambda'|^{s+1}},\ \mathrm{Re}\, s>1, \tag{3.148}$$

由 $N(\mathfrak{A})=a>0$，即知(3.148)成为

$$I(s,\ \mathfrak{A}) = -is\,d^{\frac{s}{2}}\frac{\Gamma\left(\frac{s+1}{2}\right)^2}{\Gamma(s+1)}$$

$$\cdot\sum_{\lambda\in\mathfrak{A}/\varepsilon_+}'\frac{\chi(N(\lambda)/N(\mathfrak{A}))\mathrm{sign}N(\lambda)}{|N(\lambda)/N(\mathfrak{A})|^s}$$

$$= -2isd^{\frac{s}{2}}\frac{\Gamma\left(\frac{s+1}{2}\right)^2}{\Gamma(s+1)}$$

$$\cdot\left(\sum_{\substack{\lambda\in\mathfrak{A}/\varepsilon_+\\ \lambda>0}}\frac{\chi\left(\frac{N(\lambda)}{N(\mathfrak{A})}\right)}{\left(\frac{N(\lambda)}{N(\mathfrak{A})}\right)^s}-\chi(-1)\sum_{\substack{\lambda\in\mathfrak{A}^*/\varepsilon_+\\ \lambda>0}}\frac{\chi\left(\frac{N(\lambda)}{N(\mathfrak{A}^*)}\right)}{\left(\frac{N(\lambda)}{N(\mathfrak{A}^*)}\right)^s}\right),$$

$$\mathrm{Re}\, s>1, \tag{3.149}$$

这里的 $\mathfrak{A}^*=\sqrt{d}\,\mathfrak{A}$ 与 $\mathfrak{A}$ 属于同一个广类。

令 $\mathfrak{A}$ 与 $\mathfrak{A}^*$ 所属的狭义理想类分别为 A 与 A^*，则由(3.149)以及 §2.2 的定义(3.116)，即得

$$\tilde{L}(s,\ \chi|A)-\chi(-1)\tilde{L}(s,\ \chi|A^*)$$

$$=\frac{i\Gamma(s+1)d^{-\frac{s}{2}}}{2s\Gamma\left(\frac{s+1}{2}\right)^2}I(s,\ \mathfrak{A}),\ \mathrm{Re}\, s>1. \tag{3.150}$$

以下来计算 $I(s,\ \mathfrak{A})$ 在 $s=1$ 处的极限公式。对 $\mathrm{Re}\, s>1$，有

$$E(s,\ Z,\ \mathfrak{A})=2Y^s\sum_{m=1}^{\infty}\frac{\chi(am^2)}{m^{2s}}$$

$$+2\sum^{\infty}\sum_{m=-\infty}^{+\infty}\frac{\chi(f(m,\ n))Y^s}{|m+nZ|^{2s}}$$

$$=2Y^s\chi(a)E_0+2Y^s\sum_{n=1}^{\infty}E_n, \tag{3.151}$$

其中

$$f(m,\ n)=am^2+bmn+cn^2,$$

$$E_0=\zeta(2s)\prod_{p|k}(1-p^{-2s})\ (p\ \text{表有理素数}),$$

$$E_n=E_n(X)=\sum_{m=-\infty}^{+\infty}\frac{\chi(f(m,\ n))}{((m+nX)^2+(nY)^2)^s}. \tag{3.152}$$

注意以上均已设 $\mathrm{Re}\, s>1$，以下不再一一声明。

对固定的 $Y>0$ 以及 $s(\mathrm{Re}\, s>1)$，$E_n(X)$ 是 X 的周期为 k 的周期函数。于是

$$E_n=E_n(X)=\sum_{u=-\infty}^{+\infty}a_u e^{2\pi iuX/k}, \tag{3.153}$$

其中

$$a_u=\frac{1}{k}\int_0^k E_n(X)e^{-2\pi iuX/k}dX$$

$$=\frac{1}{k}\sum_{m=-\infty}^{+\infty}\chi(f(m,n))\int_0^k\frac{e^{-2\pi iuX/k}dX}{((m+nX)^2+(nY)^2)^s}$$

$$=\frac{1}{k}\sum_{m(\bmod kn)}\chi(f(m,n))$$

$$\times\sum_{m_1=-\infty}^{+\infty}\int_0^k\frac{e^{-2\pi iuX/k}dX}{((m+n(X+km_1))^2+(nY)^2)^s}$$

$$=\frac{1}{k}\sum_{m(\bmod n)}\chi(f(m,n))$$

$$\cdot\int_{-\infty}^{+\infty}\frac{e^{-2\pi iuX/k}}{((m+nX)^2+n^2Y^2)^s}dX.$$

在上述积分中，令 $m+nX\mapsto nXY$，则有

$$a_u=\frac{Y^{1-2s}n^{-2s}}{k}\sum_{m(\bmod kn)}\chi(f(m,n))e^{2\pi ium/(kn)}$$

$$\cdot\int_{-\infty}^{+\infty}\frac{e^{-2\pi iuXY/k}}{(1+X^2)^s}dX,$$

用(3.129)，即得

$$a_0=\frac{Y^{1-2s}n^{-2s}}{k}\cdot\frac{\sqrt{\pi}\,\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)}\sum_{m(\bmod kn)}\chi(f(m,n)),\tag{3.154}$$

以及 $u\neq 0$ 时，

$$a_u=\frac{Y^{-1-2s}n^{-2s}}{k}\cdot\frac{2\sqrt{\pi}}{\Gamma(s)}\left(\frac{\pi|u|Y}{k}\right)^{s-\frac{1}{2}}$$

$$\cdot K_{s-\frac{1}{2}}\left(\frac{2\pi|u|Y}{k}\right)\sum_{m(\bmod kn)}\chi(f(m,n))e^{2\pi ium/(kn)}.\tag{3.155}$$

再用

$$\sum_{m(\bmod kn)}\chi(f(m,n))e^{2\pi ium/(kn)}$$

$$=\begin{cases} n\sum_{m(\bmod k)}\chi(f(m,n))e^{2\pi ium/(kn)}, & \text{如 } n\mid u;\\ 0, & \text{如 } n\nmid u.\end{cases}$$

即由(3.151)—(3.155)可得

$$E(s,Z,\mathfrak{A})=2Y^s\chi(a)\zeta(2s)\prod_{p\mid k}(1-p^{2s})$$

$$+\frac{2\sqrt{\pi}\,\Gamma\left(s-\frac{1}{2}\right)}{k\Gamma(s)}Y^{1-s}\sum^{\infty}n^{1-2s}\sum_{m(\bmod k)}\chi(f(m,n))$$

$$+\frac{8\pi^s}{\Gamma(s)}k^{-s-\frac{1}{2}}Y^{\frac{1}{2}}\sum_{u=1}^{\infty}u^{s-\frac{1}{2}}K_{s-\frac{1}{2}}\left(\frac{2\pi uY}{k}\right)$$

$$\cdot\sum_{1<n|u}n^{1-2s}\sum_{m(\bmod k)}\chi(f(m,n))\cos\frac{2\pi u}{k}\left(\frac{m}{n}+X\right)$$

$$=I_1+I_2+I_3. \tag{3.156}$$

易知

$$\frac{\partial I_1}{\partial Z}=2sY^{s-1}(2i)^{-1}\chi(a)\zeta(2s)\prod_{p|k}(1-p^{-2s}) \tag{3.157}$$

当 $\mathrm{Re}s>\frac{1}{2}$ 时，是解析的，而当 $s\to1$ 时，对 $Z\in\Gamma$，一致地有

$$\frac{\partial I_1}{\partial Z}=\frac{\pi^2}{6i}\chi(a)\prod_{p|k}(1-p^{-2})+O(|s-1|),\ s\to1. \tag{3.158}$$

又用 §1.3 的 Hurwitz ζ 函数，即有

$$\frac{\partial I_2}{\partial Z}=\frac{2\sqrt{\pi}\,\Gamma\left(s-\frac{1}{2}\right)}{k\Gamma(s)}\frac{1-s}{2i}Y^{-s}$$

$$\cdot\sum^{\infty}n^{-2s}\sum_{m(\bmod k)}\chi(f(m,n))$$

$$=\frac{2\sqrt{\pi}\,\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)k^{2s}}\frac{1-s}{2i}Y^{-s}$$

$$\cdot\sum_{1<m,n<k}\chi(f(m,n))\zeta\left(2s-1,\frac{n}{k}\right), \tag{3.159}$$

于是 $\frac{\partial I_2}{\partial Z}$ 是 $\mathrm{Re}s>\frac{1}{2}$ 时的解析函数，且当 $s\to1$ 时，对 $Z\in\Gamma$ 一致地有

$$\frac{\partial I_2}{\partial Z}=\frac{i\pi}{2k^2}\sum_{m,n(\bmod k)}\chi(f(m,n))+O(|s-1|),s\to1. \tag{3.160}$$

又对 Bessel 函数 K_ν 有(可参考[20]p.967 与 p.970)

$$-2\frac{dK_{s-\frac{1}{2}}(W)}{dW}=K_{s-\frac{3}{2}}(W)+K_{s+\frac{1}{2}}(W),$$

$$K_{\pm\frac{1}{2}}(W)=\sqrt{\frac{\pi}{2W}}e^{-W},\quad K_{\frac{3}{2}}(W)=\sqrt{\frac{\pi}{2W}}\left(1+\frac{1}{W}\right)e^{-W},$$

再用 K_ν 的阶估计，仿照上一小节虚二次域的情况，可以证明 $\frac{\partial I_3}{\partial Z}$ 是 $\operatorname{Re} s>0$ 时的解析函数，且当 $s\to1$ 时，对 $Z\in\Gamma$，一致地有

$$\begin{aligned}\frac{\partial I_3}{\partial Z}=&\frac{8\pi}{k^{3/2}}\sum_{u=1}^{\infty}\sqrt{u}\sum_{1<n\mid u}n^{-1}\sum_{m(\bmod k)}\chi(f(m,n))\\&\times\left(\frac{Y^{-\frac{1}{2}}}{4i}K_{\frac{1}{2}}\left(\frac{2\pi uY}{k}\right)\cos\frac{2\pi u}{k}\left(\frac{m}{n}+X\right)\right.\\&-\frac{Y^{\frac{1}{2}}}{2}\left(K_{-\frac{1}{2}}\left(\frac{2\pi uY}{k}\right)+K_{\frac{3}{2}}\left(\frac{2\pi uY}{k}\right)\right)\\&\times\frac{2\pi u}{k}\cdot\frac{1}{2i}\cos\frac{2\pi u}{k}\left(\frac{m}{n}+X\right)\\&\left.-Y^{\frac{1}{2}}K_{\frac{1}{2}}\left(\frac{2\pi uY}{k}\right)\frac{\pi u}{k}\sin\frac{2\pi u}{k}\left(\frac{m}{n}+X\right)\right)\\&+O(|s-1|),\quad s\to1\\=&\frac{\pi}{k}\sum_{u=1}^{\infty}\frac{2\pi ui}{k}e^{2\pi iuZ/k}\\&\times\sum_{1<n\mid u}n^{-1}\sum_{m(\bmod k)}\chi(f(m,n))e^{2\pi ium/(kn)}\\&+O(|s-1|),\quad s\to1.\end{aligned}\tag{3.161}$$

由(3.156)、(3.157)和(3.159)，以及上述关于 $\frac{\partial I_3}{\partial Z}$ 在 $\operatorname{Re}s>0$ 时解析的论述，我们已给出了 $\frac{\partial}{\partial Z}E(s,Z,\mathfrak{A})$ 在 $\operatorname{Re}s>0$ 时的解析开拓，它在 $\operatorname{Re}s>\frac{1}{2}$ 中是解析的，并且由(3.156)、(3.158)、(3.160)及(3.161)可知，当 $s\to1$ 时，对 $Z\in\Gamma$ 一致地有

$$\begin{aligned}\lim_{s\to1}\frac{\partial E(s,Z,\mathfrak{A})}{\partial Z}=&\frac{\pi^2}{6i}\chi(a)\prod_{p\mid k}(1-p^{-2})\\&-\frac{\pi Y^{-1}}{2ik^2}\sum_{m,n(\bmod k)}\chi(f(m,n))\\&+\frac{2\pi}{k}\sum_{u=1}^{\infty}\left(\frac{d}{dZ}e^{2\pi iuZ/k}\right)\sum_{1<n\mid u}n^{-1}\end{aligned}$$

$$\times \sum_{m(\bmod k)} \chi(f(m, n)) e^{2\pi i u m/(kn)}, \tag{3.162}$$

这样，我们得到了 $I(s, \mathfrak{A})$ 在 $\operatorname{Re} s>0$ 时的解析开拓，它在 $\operatorname{Re} s > \frac{1}{2}$ 中是解析的，且由(3.162)可得

$$\begin{aligned} I(1, \mathfrak{A}) &= \lim_{s\to 1} I(s, \mathfrak{A}) = \int_{\Gamma(Z_0, Z_0^*)} \lim_{s\to 1} \frac{\partial E(s, Z, \mathfrak{A})}{\partial Z} dZ \\ &= \frac{\pi^2}{6i} \chi(a) \prod_{p\mid k} (1-p^{-2})(Z_0^* - Z_0) \\ &\quad - \frac{\pi}{2ik^2} \sum_{m,n(\bmod k)} \chi(f(m, n)) \int_{\Gamma(Z_0, Z_0^*)} \frac{dZ}{y} \\ &\quad + \frac{2\pi}{k} \sum_{u=1}^{\infty} e^{2\pi i u Z/k} \sum_{1<n\mid u} n^{-1} \sum_{m(\bmod k)} \chi(f(m, n)) \\ &\quad \times e^{2i\pi u m/(kn)} \Big|_{Z = Z_0}^{Z = Z_0^*}, \end{aligned} \tag{3.163}$$

圆周 Γ 的圆心是 $\left(\frac{b}{2a}, 0\right)$，半径 $R = \frac{\sqrt{d}}{2a}$。令在 Γ 上

$$Z = \frac{b}{2a} + Re^{i\theta},$$

则有

$$\begin{aligned} \int_{\Gamma(Z_0, Z_0^*)} \frac{dZ}{Y} &= \int_{\theta_0}^{\theta_0^*} \frac{ie^{i\theta} d\theta}{\sin\theta} = (i\log\sin\theta - \theta) \Big|_{\theta=\theta_0}^{\theta=\theta_0^*} \\ &= i\log\frac{Y_0^*}{Y_0} - (\theta_0^* - \theta_0) = \theta_0 - \theta_0^*, \end{aligned}$$

这里 θ_0^*，θ_0 分别为 Z_0^*，Z_0 和圆心连线与正实轴所夹的角，于是 $\theta - \theta_0^*$ 是 $\Gamma(Z_0, Z_0^*)$ 的圆心角 φ。这里用到了(3.139)—(3.143)，以及 $X_0^* > X_0$。从而由

$$|Z_0 - Z_0^*| = |X_0 - X_0^*| = \frac{\sqrt{d}}{a} \frac{\varepsilon_+^2 - \varepsilon_+^{-2}}{\varepsilon_+^2 + \varepsilon_+^{-2}},$$

$$Y_0 = Y_0^* = \frac{\sqrt{d}}{2a} \frac{2}{\varepsilon_+^2 + \varepsilon_+^{-2}},$$

可得

$$\cos\frac{\varphi}{2} = \frac{2}{\varepsilon_+^2 + \varepsilon_+^{-2}}, \quad \sin\frac{\varphi}{2} = \frac{\varepsilon_+^2 - \varepsilon_+^{-2}}{\varepsilon_+^2 + \varepsilon_+^{-2}}, \tag{3.164}$$

以及

$$\int_{\Gamma(Z_0, Z_0^*)} \frac{dZ}{Y} = \varphi. \tag{3.165}$$

命

$$X_{\mathfrak{A}} = \frac{\sqrt{d}}{2a} \cdot \frac{\varepsilon_+^2 - \varepsilon_+^{-2}}{\varepsilon_+^2 + \varepsilon_+^{-2}},$$

$$Y_{\mathfrak{A}} = \frac{\sqrt{d}}{2a} \cdot \frac{2}{\varepsilon_+^2 + \varepsilon_+^{-2}}, \quad Z_{\mathfrak{A}} = X_{\mathfrak{A}} + iY_{\mathfrak{A}}. \tag{3.166}$$

则有

$$Z_{\mathfrak{A}} = \frac{\sqrt{d}}{2a}\left(\frac{\varepsilon_+ + i\varepsilon_+^{-1}}{|\varepsilon_+ + i\varepsilon_+^{-1}|}\right)^2 = \frac{\sqrt{d}}{2a} e^{i\varphi}_{\mathfrak{A}}, \tag{3.167}$$

$$\cos\varphi_{\mathfrak{A}} = \frac{\varepsilon_+^2 - \varepsilon_+^{-2}}{\varepsilon_+^2 + \varepsilon_+^{-2}}, \quad \sin\varphi_{\mathfrak{A}} = \frac{2}{\varepsilon_+^2 + \varepsilon_+^{-2}}, \tag{3.168}$$

$$X_0^* = \frac{b}{2a} + X_{\mathfrak{A}}, \quad X^0 = \frac{b}{2a} - X_{\mathfrak{A}}, \quad Y_0^* = Y_0 = Y_{\mathfrak{A}}, \tag{3.169}$$

$$\varphi = \frac{\pi}{2} - \varphi_{\mathfrak{A}}. \tag{3.170}$$

那么由(3.163)～(3.170)可得

$$\begin{aligned} I(1, \mathfrak{A}) = &-\frac{i\pi^2}{3}\chi(a)\prod_{p|k}(1-p^{-2})X_{\mathfrak{A}} \\ &+ \frac{i\pi}{k^2}\left(\frac{\pi}{2} - \varphi_{\mathfrak{A}}\right)\sum_{m,n(\bmod k)}\chi(f(m, n)) \\ &+ \frac{2\pi}{k}\sum_{u=1}^{\infty}\left(e^{2\pi i u Z/k}\Big|_{Z=-\bar{Z}_{\mathfrak{A}}}^{Z=Z_{\mathfrak{A}}}\right)\cdot\sum_{1\le n|u} n^{-1} \\ &\times \sum_{m(\bmod k)}\chi(f(m, n))\exp\left(\frac{2\pi i u}{k}\left(\frac{m}{n} + \frac{b}{2a}\right)\right), \end{aligned} \tag{3.171}$$

由(3.150)及以上的讨论可知，我们已给出(3.150)的左边当 Re $s>0$ 时的解析开拓，它在 Re $s>\frac{1}{2}$ 中是解析的，这就给出了下述定理 2.4 的前一部分，而把 (3.171) 代入 (3.150) 就给出了定理 2.4 的 $j=1$ 时的后一部分。

定理 2.4 设 $\mathfrak{A} = \left[a, \frac{-b+\sqrt{d}}{2}\right]$为 $K = Q(\sqrt{d})$ 的一个

整理想，有理整数 a, b, c 满足 $g.c.d.(a, b, c)=1$, $a>0$, $b^2-4ac=d$, d 为实二次域 $K=Q(\sqrt{d})$ 的判别式。k 为一个正整数，χ 为 $\bmod k$ 的一个 Dirchlet 特征。那么对于 $\mathfrak{A}$ 与 $\mathfrak{A}^*=\sqrt{d}\,\mathfrak{A}$ 所属的狭义理想类 A 与 A^*，函数

$$\tilde{L}(s, \chi|A)-\chi(-1)\tilde{L}(s, \chi|A^*)$$

在 $\operatorname{Re} s>\frac{1}{2}$ 中解析，并且在 $s=1$ 处，有下列极限公式：

$$\begin{aligned}
&\frac{j}{2}\lim_{s\to1}(\tilde{L}(s, \chi|A)-\chi(-1)\tilde{L}(s, \chi|A^*))\\
&=\frac{\pi^2}{12\sqrt{d}}\chi(a)\prod_{p|k}(-p^{-2})\operatorname{Re} z_{\mathfrak{A},j}\\
&\quad-\frac{\pi}{4k^2}\,\frac{\frac{\pi}{2}-\varphi_{\mathfrak{A},j}}{\sqrt{d}}\sum_{m,n(\bmod k)}\chi(am^2+bmn+cn^2)\\
&\quad+\frac{\pi i}{2k\sqrt{d}}\sum_{u=1}^{\infty}\left(e^{2\pi iuz/k}\Big|_{z=-\bar{z}_{\mathfrak{A},j}}^{z=z_{\mathfrak{A},j}}\right)\sum_{1<n|u}n^{-1}\\
&\quad\times\sum_{m(\bmod k)}\chi(am^2+bmn+cn^2)\exp\left(\frac{2\pi u}{k}\left(\frac{b}{2a}+\frac{m}{n}\right)\right),
\end{aligned}$$

这里 j 是任一个正整数，p 表有理素数。

$$z_{\mathfrak{A},j}=\frac{\sqrt{d}}{2a}\left(\frac{\varepsilon_+^j+i\varepsilon_+^{-j}}{|\varepsilon_+^j+i\varepsilon_+^{-j}|}\right)^2,$$

$$\varphi_{\mathfrak{A},j}=\arg z_{\mathfrak{A},j},\quad 0>\varphi_{\mathfrak{A},j}<\frac{\pi}{2}.$$

证明 $j=1$ 时，已由上述的推理证得。此时 $z_{\mathfrak{A},1}=Z_{\mathfrak{A}}$。对一般的正整数 j，用 ε_+^j 代替 ε_+，即可由上述推理同样得知，本定理仍然成立，只要注意到 $N(\varepsilon_+)=1$，并且在推理过程中，下列有关的求和公式成立：

$$\sum_{/\varepsilon_+^j}=j\sum_{/\varepsilon_+},$$

详细过程不再赘述了。

现在我们来看几个特例。

首先取 χ 为实特征，这时定理 2.4 中的极限公式的左边显然

是一个实数。于是在右边的第三项，可把 exp 换为 cos。

其次取 $k=1$。记 χ 为 χ_0，这时有

$$\frac{j}{2}\lim_{s\to 1}(\tilde{Z}(s,\ \chi_0|A)-\tilde{Z}(s,\ \chi_0|A^*))$$

$$=-\frac{\pi}{4\sqrt{d}}\left(\frac{\pi}{2}-\varphi_{\mathfrak{A},j}\right)$$

$$+\frac{\pi}{2\sqrt{d}}\operatorname{Im}\Big(\log\eta\Big(z_{\mathfrak{A},j}+\frac{b}{2a}\Big)$$

$$+\log\eta\Big(z_{\mathfrak{A},j}-\frac{b}{2a}\Big)\Big),\tag{3.172}$$

其中 η 是 Dedekind η-函数。

再取 $k|d$，且取 χ 为 mod k 的实原特征，再设 $g.c.d.(a,\ d)=1$，且 k 奇，易见这时有(注意 $n|u$)

$$\sum_{m(\bmod k)}\chi\cdot(am^2+bmn+cn^2)\cos\left(\frac{2\pi u}{k}\left(\frac{b}{2a}+\frac{m}{n}\right)\right)$$

$$=\chi(a)\sum_{m(\bmod k)}\chi((2am+bn)^2-dn^2)\cos\left(\frac{2\pi u}{k}\left(\frac{b}{2a}+\frac{m}{n}\right)\right),$$

命 $a_1\in\mathbb{Z}$，使 $2aa_1\equiv 1(\bmod k)$，令 $m\mapsto a_1m-a_1bn$，再用 Ramanujan 和的公式(见 Hardy 与 Wright[25]p.237)，即知上式

$$=\chi(a)\sum_{m(\bmod k)}\chi^2(m)\cos\left(\frac{2\pi u}{k}\left(\frac{1-2aa_1}{2a}b+\frac{a_1m}{n}\right)\right)$$

$$=\chi(a)\operatorname{Re}\left(e^{2\pi iu(1-2aa_1)/(2ak)}\sum_{\substack{m(\bmod k)\\ g.c.d.(m,k)=1}}e^{2\pi i\frac{u}{n}\frac{m}{k}}\right)$$

$$=\chi(a)\sum_{\substack{1\leqslant m|k\\ m|\frac{u}{n}}}m\mu\left(\frac{k}{m}\right)\cos\frac{2\pi u(1-2aa_1)b}{2ak},$$

这样由定理 2.4 得到下面的引理。

引理 2.2　设 d 为一个正的基本判别式，正奇数 $k|d$，χ 为 mod k 的实原特征，以及 $g.c.d.(a,\ d)=1$。则在定理 2.4 的假设下，有

$$\frac{j}{2}\lim_{s\to 1}(\tilde{Z}(s,\ \chi|A)-\chi(-1)\tilde{Z}(s,\ \chi|A^*))$$

$$= \frac{\pi}{2\sqrt{d}}\chi(a)\sum_{1<m|k}\frac{\mu(m)}{m}\left(\operatorname{Im}\log\eta\left(\frac{z_{\mathfrak{A},j}+\frac{1-2aa_1}{2a}b}{m}\right)\right.$$

$$\left.+\operatorname{Im}\log\eta\left(\frac{z_{\mathfrak{A},j}-\frac{1-2aa_1}{2a}b}{m}\right)\right)$$

$$-\frac{\pi}{4\sqrt{d}}\left(\frac{\pi}{2}-\varphi_{\mathfrak{A},j}\right)\frac{\varphi(k)}{k}\chi(a),$$

其中 $a_1\in\mathbb{Z}$，满足 $2aa_1\equiv 1\pmod{k}$，η 是 Dedekind η-函数。

证明 第二项的计算用了第二章 §1.6 的定理 1.8，其余显然。

同样可得下面的引理。

引理 2.3 设 d 为一个正的基本判别式，正偶数 $k|d$，χ 为 $\bmod k$ 的实原特征，且 $g.c.d.(a, d)=1$。则在定理 2.4 的假定下，有：

$$\frac{j}{2}\lim_{s\to1}(\tilde{L}(s,\chi|A)-\chi(-1)\tilde{L}(s,\chi|A^*))$$

$$=-\frac{\pi}{4\sqrt{d}}\left(\frac{\pi}{2}-\varphi_{\mathfrak{A},j}\right)\frac{\varphi(k)}{k}\chi(a)$$

$$+\frac{\pi}{2\sqrt{d}}\chi(a)\sum_{1<m|k}\frac{\mu(m)}{m}\left(\operatorname{Im}\log\eta\left(\frac{z_{\mathfrak{A},j}+\frac{1-aa_1}{2a}b}{m}\right)\right.$$

$$\left.+\operatorname{Im}\log\eta\left(\frac{z_{\mathfrak{A},j}-\frac{1-aa_1}{2a}b}{m}\right)\right),$$

其中 $a_1\in\mathbb{Z}$，满足 $aa_1\equiv 1\pmod{d}$，η 是 Dedekind η-函数。

特别的取 $k=4$ 或 8，即有下面的引理。

引理 2.4 设 $d=kd_1$ 为基本判别式，其中 $k=4$ 或 8，d_1 为正奇数，χ 为 $\bmod k$ 的实原特征，即

$$\chi(*)=\left(\frac{-4}{*}\right),\ \left(\frac{\pm 8}{*}\right)$$

(Kronecker 符号)再设 $\mathfrak{A}=O_K=[1]$，即 $a=1$，$b=0$，$c=-\frac{d}{4}$。

则在定理 2.4 的假定下，有：

$$\frac{j}{2}\lim_{s\to 1}(\tilde{L}(s,\ \chi|A)-\chi(-1)\tilde{L}(s,\ \chi|A^*))$$

$$=-\frac{\pi}{8\sqrt{d}}\left(\frac{\pi}{2}-\varphi_{\mathfrak{A},\mathfrak{f}}\right)$$

$$+\frac{\pi}{2\sqrt{d}}\left(2\operatorname{Im}\log\eta(z_{\mathfrak{A},\mathfrak{f}})-\operatorname{Im}\log\eta\left(\frac{z_{\mathfrak{A},\mathfrak{f}}}{2}\right)\right),$$

其中 η 为 Dedekind η-函数。

本章评注

1. 极限公式的经典内容除上述已列的 C.L.Siegel 的书以外，还可参考 D.Zagier[113]。

2. 定理 1.2 采自参考文献[59]，它将在第六章和第七章中发挥作用。

3. §2.2 与 §2.4 的内容采自参考文献[60]。

4. §2.3 中所用方法与 H.stark[96] 的略有不同。

第 4 章

Gauss 类数猜想的一般性讨论

由第二章知道,对一个二次域 $K=Q(\sqrt{d})$, 其中 d 为K的判别式,域 K 的类数的大小与 $L(1, \chi_d)$密切相关,在实二次域里,还与正则子 $\log\varepsilon$(ε 是 K 的基本单位)密切相关。在本章中,我们首先讨论 $L(1, \chi_d)$的阶,特别是 Siegel 定理及其改进,以便明了 Gauss 类数问题困难之所在;然后对实二次域讨论正则子与连分数展开式周期长度的关系,这样才能明白为什么实二次域的类数问题远为困难得多。本章也是以后两章的准备,有了这些准备之后,才能深入地研究 Gauss 类数问题。在本章的末尾再介绍一下 Euclid 域。

§1 Dirichlet L-函数的零点分布和阶的估计

1.1 Dirichlet L-函数的一般讨论

本小节中列举 Dirichlet L-函数的一些性质(可参考:潘承洞与潘承彪著《解析数论基础》)。

设 k 为一个正整数,对 mod$k$ 的特征 χ, 考虑下列的 Dirichlet L-函数:

$$L(s, \chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s},\ s=\sigma+it,\ \mathrm{Re}\,s=\sigma>1.$$

当 $k=1$ 时,$L(s, \chi)$即为 Riemann ζ 函数 $\zeta(s)$。

引理 1.1 (1) Riemann ζ 函数

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\ s=\sigma+it,\ \mathrm{Re}\,s=\sigma>1,$$

可以解析开拓到整个 s 平面,成为 s 的一个半纯函数,它仅有的奇

点是一阶极点 $s=1$。它在 $s=1$ 处的 Laurent 展式是

$$\zeta(s)=\frac{1}{s-1}+\sum_{n=0}^{\infty}(-1)^n\frac{\gamma_n}{n!}(s-1)^n,$$

其中

$$\gamma_0=\gamma=\lim_{N\to\infty}\left(\sum_{m=1}^{N}\frac{1}{m}-\log N\right)$$

是 Euler 常数，而 $n\geqslant 1$ 时，

$$\gamma_n=\lim_{N\to\infty}\left(\sum_{m=1}^{N}\frac{(\log m)^n}{m}-\frac{(\log N)^{n+1}}{n+1}\right),$$

$\gamma_n(n\geqslant 0)$ 统称为 Stieltjes 常数。

(2) $\zeta(s)$ 满足函数方程

$$\xi(s)\overset{\text{def}}{=}\frac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)=\xi(1-s),$$

并且 $\xi(s)$ 是一阶的整函数，它的无穷多个零点，全在临界竖长条 $0<\sigma<1$ 中，$\xi(0)=\frac{1}{2}$。

因此 $\zeta(s)$ 除在 $s=-2n(n\in\mathbb{Z},\ n\geqslant 1)$ 处有一阶零点（这些零点均称为显然零点）以外，它的其余的无穷多个零点 ρ（这些零点称为非显然零点），全在临界竖长条 $0<\sigma<1$ 中：

$$\rho=\beta+i\alpha,\ 0<\beta<1,$$

同时还有：$\operatorname{Im}\rho=\alpha\neq 0$，且 $\rho,\ \bar{\rho},\ 1-\rho,\ 1-\bar{\rho}$ 同为零点。

(3) 当 $s\neq\rho,\ +1,\ -2n(n=1,\ 2,\ \cdots)$ 时，有：

$$\frac{\zeta'(s)}{\zeta(s)}=\frac{-1}{s-1}+B+\frac{\gamma}{2}+\frac{1}{2}\log\pi+\sum_{\rho}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right)+\sum^{\infty}\left(\frac{1}{s+2n}-\frac{1}{2n}\right),$$

其中右边的两个级数分别在任一个不包含 $\zeta(s)$ 的任何非显然零点 ρ 与显然零点 $-2n$ 的有界闭区域上一致收敛，而常数

$$B=-\sum_{\rho}\operatorname{Re}\frac{1}{\rho}=-1-\frac{\gamma}{2}+\frac{1}{2}\log(4\pi)=-0.023095\cdots.$$

(4) Riemann 猜想(RH) $\zeta(s)$ 的所有非显然零点全在

$$\operatorname{Re}s=\sigma=\frac{1}{2}$$

这条直线上。

(5) $\zeta(0)=-\frac{1}{2}$, $\zeta(1-2n)=\frac{(-1)^n}{2n}B_n(n=1,\ 2,\ \cdots)$,

$$\zeta(2n)=2^{2n-1}\pi^{2n}\frac{B_n}{(2n)!}(n=1,\ 2,\ \cdots),$$

其中 B_n 是 Bernoulli 数：

$$\frac{z}{e^z-1}=1-\frac{1}{2}z+\sum^{\infty}(-1)^{n-1}B_n\frac{z^{2n}}{(2n)!},$$

特别的有

$$B_1=\frac{1}{6},\ B_2=\frac{1}{30},\ B_3=\frac{1}{42},\ B_4=\frac{1}{30},$$

$$B_5=\frac{5}{66},\ B_6=\frac{691}{2730},\ B_7=\frac{7}{6},\ B_8=\frac{3617}{510},$$

$$B_9=\frac{43867}{798},\ B_{10}=\frac{174611}{330},\ \cdots$$

(6) $\zeta(s)$的非显然零点 $\rho=\beta+i\alpha$, 以$|\alpha|$由小到大的顺序排列的最初五十万个，都有 $\beta=\frac{1}{2}$, 其中最初的二十个是

$$\rho_j=\frac{1}{2}\pm\alpha_j(1\leqslant j\leqslant 10),$$

这些 α_j 的值如下表所示：

$\alpha_1=14.134725$, $\alpha_2=21.022040$,

$\alpha_3=25.010856$, $\alpha_4=30.424878$,

$\alpha_5=32.935057$, $\alpha_6=37.586176$,

$\alpha_7=40.918720$, $\alpha_8=43.327073$,

$\alpha_9=48.005150$, $\alpha_{10}=49.773832$.

注意上述α_j的数值除在小数点之后的第六位有点小出入之外，全是准确的。上述数值取自 H.M.Edwards《Riemann's zeta Function》p.96。

引理 1.2 (1) 设 χ 为 mod k 的特征，其中 k 为一个正整数，则 $L(s,\ \chi)$可以解析开拓到整个 s 平面。当 χ 不是 mod k 的主特征时，$L(s,\ \chi)$成为一个整函数；当 χ 是 mod k 的主特征时，$L(s,\ \chi)=\zeta(s)\prod\limits_{p|k}(1-p^{-s})$ (p 表素数)，从而此时 $L(s,\ \chi)$ 成为一个半

纯函数，它仅有的奇点是一阶极点 $s=1$，相应的残数是 $\frac{\varphi(k)}{k}$，$\varphi(k)$是 Euler 函数。

(2) 如 $k\geqslant 3$，且 χ 是 mod k 的原特征，则有函数方程

$$\xi(s,\ \chi)\overset{\text{def}}{=}\left(\frac{k}{\pi}\right)^{\frac{1}{2}(s+\delta_\chi)}\Gamma\left(\frac{s+\delta_\chi}{2}\right)L(s,\ \chi)$$

$$=\frac{\sqrt{k}}{\tau(\bar{\chi})}i^{\delta_\chi}\xi(1-s,\ \bar{\chi}),$$

其中$\tau(\bar{\chi})=\sum\limits_{n=1}^{k}\bar{\chi}(n)e^{2\pi in/k}$ 为 Gauss 和；$\delta_\chi=\frac{1}{2}(1-\chi(-1))=0$或 1，视 $\chi(-1)=1$ 或 -1 而定，并且 $\xi(s,\ \chi)$是一阶整函数，它的无穷多个零点全在临界竖长条 $0<\sigma<1$ 上。

因此，这时的 $L(s,\ \chi)$除在 $s=-(2n+\delta_\chi)\ (n=0,\ 1,\ 2,\ \cdots)$处有一阶零点（这些零点均称为显然零点）以外，它的其余的无穷多个零点（这些零点均称为非显然零点）ρ_χ 全在临界竖长条 $0<\sigma<1$ 上：

$$\rho_\chi=\beta_\chi+i\alpha_\chi,\quad 0<\beta_\chi<1.$$

ρ_χ 与 $1-\bar{\rho}_\chi$ 同为零点，如 χ 还为实特征，则 ρ_χ 与$\bar{\rho}_\chi$ 同为零点。

(3) 在(2)的假定下，当 $s\neq\rho_\chi,\ -(2n+\delta_\chi)\ (n=0,\ 1,\ 2,\ \cdots)$时，有

$$\frac{L'}{L}(s,\ \chi)=D+\frac{1}{s+\delta_\chi}+\sum_{n=1}^{\infty}\left(\frac{1}{s+\delta_\chi+2n}-\frac{1}{2n}\right)$$

$$+\sum_{\rho_\chi}\left(\frac{1}{s-\rho_\chi}+\frac{1}{\rho_\chi}\right),$$

其中右边的两个级数分别在任一个不包含 $L(s,\ \chi)$ 的显然零点和非显然零点的有界闭区域上一致收敛；常数

$$D=B(\chi)+\frac{1}{2}\gamma+\frac{1}{2}\log\frac{\pi}{k},$$

而 $B(\chi)$为仅依赖于 χ 的一个常数，它具有性质：

$$B(\bar{\chi})=\overline{B(\chi)},\ \operatorname{Re}B(\chi)=-\sum_{\rho_\chi}\operatorname{Re}\frac{1}{\rho_\chi}<0.$$

从而有：

$$-\mathrm{Re}\frac{L'}{L}(s,\ \chi)=\frac{1}{2}\log\frac{k}{\pi}+\frac{1}{2}\mathrm{Re}\frac{\Gamma'}{\Gamma}\left(\frac{s+\delta_\chi}{2}\right)$$
$$-\sum_{\rho_\chi}\mathrm{Re}\frac{1}{s-\rho_\chi}.$$

(4) 当 χ 为 $\bmod k$ 的非原特征时，命 χ 的导子为 f，χ_1 是与 χ 等价的 $\bmod f$ 的原特征。则由(p 表素数)

$$L(s,\ \chi)=L(s,\ \chi_1)\prod_{p\mid k}(1-\chi_1(p)p^{-s}),\ s\in\mathbb{C}$$

可知 $L(s,\ \chi)$ 比 $L(s,\ \chi_1)$ 仅可能在虚轴上多出一些零点（至多是可数无穷多个)，这些零点仍看作 $L(s,\ \chi)$ 的显然零点，这样 $L(s,\ \chi)$ 与 $L(s,\ \chi_1)$ 具有相同的非显然零点。

(5) Hecke 猜想对实特征 χ 有

$$L(s,\ \chi)\neq 0,\ \text{如}\ 0<s<1.$$

(6) 广义 Riemann 猜想 (GRH) 对任一个 Dirichlet 特征 χ, $L(s,\ \chi)$ 的所有非显然零点全在

$$\mathrm{Re}s=\sigma=\frac{1}{2}$$

这条直线上。

引理 1.3 设 k 为一个正整数，$M=\max\{k,\ k|t|,\ 10\}$。命

$$L(s,\ k)=\prod_{\chi}L(s,\ \chi),\ s=\sigma+it,$$

这里 χ 跑过所有 $\varphi(k)$ 个 $\bmod k$ 的 Dirichlet 特征。

则 $L(s,\ k)$ 在区域

$$\{s:\sigma\geqslant 1-(10\log M)^{-1}\}$$

中至多有一个零点，并且如果这个零点存在的话，一定是一阶零点，同时这个唯一可能的单零点一定是由 $\bmod k$ 的一个实的非主特征 χ 所对应的 L-函数 $L(s,\ \chi)$ 的实的单零点。如果这个实单零点确实存在的话，就称为例外零点，也称为 Siegel 零点，相应的模 k 称为例外模，χ 称为例外特征。引理 1.3 与下面的引理，可见于潘承彪与潘承洞著《解析数论基础》。

引理 1.4 设 χ_1 与 χ_2 分别是 $\bmod k_1$ 与 $\bmod k_2$ 的实原特征。且 $\chi_1\neq\chi_2$。再设 β_1 与 β_2 分别为 $L(s,\ \chi_1)$ 与 $L(s,\ \chi_2)$ 的实零点，

则有

$$\min\{\beta_1, \beta_2\}<1-(4\log M_1)^{-1}, \ M_1=\max\left\{13, \ \frac{k_1k_2}{17}\right\}.$$

由上述两个引理可得下面引理：

引理 1.5 设 $x\geqslant15$ 为一个固定的正实数。则在模小于等于 x 的所有实原特征中，仅可能有一个 $\chi\bmod k$，使得 $L(s, \chi)$ 有一个实单零点 β 满足

$$\beta>1-(10\log x)^{-1}.$$

此外，如果有实特征 $\chi_1 \bmod k_1$，$k_1\leqslant x$，使得 $L(s, \chi_1)$ 有实零点

$$\beta_1>1-(10\log x)^{-1},$$

则必然是 χ_1 的导子为 k，且 χ_1 与 χ 等价。

附注 本引理中的 k，χ，β 分别称为 x 阶的例外模、例外特征、例外零点（也称为 Siegel 零点）。

1.2 Siegel-Tatuzawa 定理

引理 1.6 设 χ 为 $\bmod k$ 的实原特征，$k\geqslant10^6$，则有：

(1) 如对 $\beta<s<1$，有 $L(s, \chi)\neq0$，其中 β 为一个满足

$$1-\beta<(12\log k)^{-1}$$

的正常数，则有

$$L(1, \chi)>1.51(1-\beta);$$

(2) 如对 $\frac{3}{4}\leqslant s<1$，有 $L(s, \chi)\neq0$，则有

$$L(1, \chi)>(1.51\log k)^{-1}.$$

证明 令二次域 $K=Q(\sqrt{d})$（d 为 K 的判别式）使

$$\chi=\chi_d=\left(\frac{d}{*}\right)$$

(Kronecker 符号)。于是 $k=|d|$，并有

$$\zeta_K(s)=\zeta(s)L(s, \chi), \ s\in C, \tag{4.1}$$

这里用到前几章的理论。由于 χ 是 $\bmod k$ 的实原特征，故 Gauss 和

$$\tau(\chi)=\sqrt{k}\, i^{\delta_\chi},$$

这样，由上小节的引理 1.2 即知，$\zeta_K(s)$ 满足下列函数方程

$$\zeta_K(1-s)=\left(\frac{\sqrt{k}}{(1+\delta_\chi)\pi}\right)^{2s-1}\left(\frac{\Gamma(s)}{\Gamma(1-s)}\right)^{\delta_\chi}\left(\frac{\Gamma\left(\frac{s}{2}\right)}{\Gamma\left(\frac{1-s}{2}\right)}\right)^{2(1-\delta_\chi)}$$

$$\cdot\zeta_K(s). \tag{4.2}$$

在 $\zeta(s)$ ($\mathrm{Re}\, s>1$) 的 Euler 求和公式($x\geqslant 1$, l 正整数)(参考潘承洞与潘承彪著《解析数论基础》)

$$\begin{aligned}\zeta(s)=&\sum_{1\leqslant n\leqslant x}\frac{1}{n^s}-\frac{x^{1-s}}{1-s}+\frac{b_1(x)}{x^s}\\&+\sum_{s=2}^{l}s(s+1)\cdots(s+j-2)\frac{b_j(x)}{x^{s+j-1}}\\&-s(s+1)\cdots(s+l-1)\int_x^{\infty}\frac{b_l(u)}{u^{s+l}}du\end{aligned} \tag{4.3}$$

中取 $s=\sigma>1$, $x=1$, $l=4$ 即有

$$\begin{aligned}\zeta(\sigma)=&\frac{\sigma}{\sigma-1}+b_1(1)+\sigma b_2(1)+\sigma(\sigma+1)b_3(1)\\&+\sigma(\sigma+1)(\sigma+2)b_4(1)\\&-\sigma(\sigma+1)(\sigma+2)(\sigma+3)\int_1^{\infty}\frac{b_4(u)}{u^{\sigma+4}}du,\end{aligned} \tag{4.4}$$

其中 $b_l(u)$ 是 Euler 函数:

$$b_1(u)=\{u\}-\frac{1}{2},$$

$$b_2(u)=\frac{1}{2}\{u\}^2-\frac{1}{2}\{u\}+\frac{1}{12},$$

$$b_3(u)=\frac{1}{6}\{u\}^3-\frac{1}{4}\{u\}^2+\frac{1}{12}\{u\},$$

$$b_4(u)=\frac{1}{24}\{u\}^4-\frac{1}{12}\{u\}^3+\frac{1}{24}\{u\}^2-\frac{1}{720},\ \cdots,$$

这里 $\{u\}$ 是 u 的小数部分, 一般地, $b_l(u)$ 是 u 的周期为 1 周期函数, 且有:

$$b_{l+1}(u)=b_{l+1}(0)+\int_0^u b_l(u)du,\ b_{2l+1}(0)=0,$$

$$b_{2l}(0)=\frac{(-1)^{l-1}B_l}{(2l)!},\quad l\geqslant 1,$$

B_l 是 Bernoulli 数。

一般地有

$$|b_{2l}(u)|\leqslant|b_{2l}(0)|,\ l\geqslant 1,\tag{4.5}$$

所以有

$$b_1(1)=-\frac{1}{2},\quad b_2(1)=\frac{1}{12},$$

$$b_3(1)=0,\ b_4(0)=b_4(1)=-\frac{1}{720},\tag{4.6}$$

$$|b_4(u)|\leqslant\frac{1}{720}.\tag{4.7}$$

因此由(4.7)，有

$$\left|-\sigma(\sigma+1)(\sigma+2)(\sigma+3)\int_1^{\infty}\frac{b_4(u)}{u^{\sigma+4}}du\right|\leqslant\frac{\sigma(\sigma+1)(\sigma+2)}{720}\tag{4.8}$$

于是由(4.4)、(4.6)与(4.8)有

$$\zeta(\sigma)=\frac{(\sigma+2)(\sigma+3)}{12(\sigma-1)}-\frac{\sigma(\sigma+1)(\sigma+2)}{360}\theta,\ \sigma>1,\ 0\leqslant\theta\leqslant 1.\tag{4.9}$$

特别有

$$\zeta\left(\frac{5}{2}\right)\leqslant\frac{11}{8},$$

从而

$$\left|\zeta_K\left(\frac{5}{2}-it\right)\right|\leqslant\zeta\left(\frac{5}{2}\right)^2\leqslant\frac{121}{64}.\tag{4.10}$$

由

$$|\Gamma(\bar{z})|=|\Gamma(z)|,\ \Gamma(z+1)=z\Gamma(z),$$

$$\sqrt{\pi}\,\Gamma(2z)=2^{2z-1}\Gamma(z)\Gamma\left(z+\frac{1}{2}\right)$$

有

$$\left|\frac{\Gamma\left(\frac{5}{2}-it\right)}{\Gamma\left(-\frac{3}{2}+it\right)}\right|=\left|\frac{3}{2}-it\right|^2\cdot\left|\frac{1}{2}-it\right|^2,$$

$$\left|\frac{\Gamma\left(\frac{5}{4}-\frac{it}{2}\right)}{\Gamma\left(-\frac{3}{4}+\frac{it}{2}\right)}\right|=\frac{1}{4}\left|\frac{3}{2}+it\right|\cdot\left|\frac{1}{2}-it\right|, \tag{4.11}$$

所以由(4.2)、(4.10)和(4.11)可得

$$\left|\zeta_K\left(-\frac{3}{2}+it\right)\right|\leqslant\frac{121k^2}{1024\pi^4}\left(\frac{9}{4}+t^2\right)\left(\frac{1}{4}+t^2\right) \tag{4.12}$$

命

$$\alpha=-\frac{3}{2}-\beta_0,\quad \frac{3}{4}\leqslant\beta_0<1,\ x=k^A,\ A>0, \tag{4.13}$$

则由(4.12)有

$$\left|\frac{6!}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty}\frac{\zeta_K(s+\beta_0)x^s ds}{s\prod_{n=2}^{6}(s+n)}\right|$$

$$\leqslant\frac{5445}{64\pi^5}k^{2-\left(\frac{3}{2}+\beta_0\right)A}\int_0^\infty\frac{\left(\frac{9}{4}+t^2\right)\left(\frac{1}{4}+t^2\right)dt}{\sqrt{(\alpha^2+t^2)\prod_{n=2}^{6}((\alpha+n)^2+t^2)}}, \tag{4.14}$$

由(4.13)可得

$$\begin{aligned}(\alpha^2+t^2)\prod_{n=2}^{6}((\alpha+n)^2+t^2)=&\left(\left(\frac{3}{2}+\beta_0\right)^2+t^2\right)\left(\left(\beta_0-\frac{1}{2}\right)^2\right.\\&\left.+t^2\right)\left(\left(\frac{3}{2}-\beta_0\right)^2+t^2\right)\left(\left(\frac{5}{2}-\beta_0\right)^2+t^2\right)\\&\times\left(\left(\frac{7}{2}-\beta_0\right)^2+t^2\right)\left(\left(\frac{9}{2}-\beta_0\right)^2+t^2\right)\\&>\left(\frac{81}{16}+t^2\right)\left(\frac{1}{16}+t^2\right)\left(\frac{1}{4}+t^2\right)\left(\frac{9}{4}+t^2\right)\\&\times\left(\frac{25}{4}+t^2\right)\left(\frac{49}{4}+t^2\right)\\&>\left(\frac{1}{4}+t^2\right)^2\left(\frac{9}{4}+t^2\right)^2\left(\frac{25}{4}+t^2\right)^2,\end{aligned} \tag{4.15}$$

其中用到

$$\left(\frac{81}{16}+t^2\right)\left(\frac{1}{16}+t^2\right)\left(\frac{49}{4}+t^2\right)-\left(\frac{1}{4}+t^2\right)$$

$$\times\left(\frac{9}{4}+t^2\right)\left(\frac{25}{4}+t^2\right)$$

$$=\frac{369}{1024}+\frac{12009}{256}t^2+\frac{69}{8}t^4>0.$$

由(4.14)与(4.15)可得

$$\left|\frac{6!}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty}\frac{\zeta_K(s+\beta_0)x^s ds}{s\prod_{n=2}^{6}(s+n)}\right|<0.175k^{2A-(\frac{3}{2}+\beta_0)}, \qquad (4.16)$$

其中用到左边

$$\leqslant\frac{5445}{64\pi^5}k^{2-(\frac{3}{2}+\beta_0)A}\int_0^{\infty}\frac{dt}{\frac{25}{4}+t^2}=\frac{5445}{64\pi^5}k^{2-(\frac{3}{2}+\beta_0)A}\cdot\frac{\pi}{5}$$

$$=\frac{1089}{64\pi^4}k^{2-(\frac{3}{2}+\beta_0)A}.$$

对正整数 $m\geqslant2$, 命

$$W(s)=\prod_{n=2}^{m}(n+s)-s\sum_{n=2}^{m}(-1)^n(n-1)\binom{m}{n}\prod_{\substack{l=2\\l\neq n}}^{m}(l+s),$$

则$W(s)$是 s 的 $m-1$ 次多项式,直接计算可得

$$W(-u)=m!,\ 如\ 0\leqslant u\leqslant m-1,\ 故\ W(s)\equiv m!,$$

即得,对任意正整数 $m\geqslant2$, 有

$$\prod_{n=2}^{m}(n+s)-s\sum_{n=2}^{m}(-1)^n(n-1)\binom{m}{n}\prod_{\substack{l=2\\l\neq n}}^{m}(l+s)=m!,\ 若 m\geqslant2,$$

从而有

$$\frac{1}{m!s}-\sum_{n=2}^{m}\frac{(-1)^n(n-1)}{n!(m-n)!(n+s)}=\frac{1}{s\prod_{n=2}^{m}(n+s)},\quad 若 m\geqslant2,$$

$$s\neq0,\ -2,\ -3,\ \cdots,\ -(m-1),\ -m, \qquad (4.17)$$

对正整数 $m\geqslant2$, 命

$$g(y)=\begin{cases}\dfrac{1}{m!}-\displaystyle\sum_{n=2}^{m}\frac{(-1)^n(n-1)}{n!(m-n)!}y^n, & 如\ 0\leqslant y\leqslant1;\\ 0, & 如\ y>1.\end{cases} \qquad (4.18)$$

易见

$$g(y)=\frac{(1-y)^m}{m!}+\frac{y(1-y)^{m-1}}{(m-1)!},\ 如\ 0\leqslant y\leqslant1,\ m\geqslant2.$$

(4.19)

故

$$g(y)\geqslant 0,\ 如\ y\geqslant 1;\ 0<g(y)\leqslant\frac{1}{m!},\ 如\ 0\leqslant y<1. \tag{4.20}$$

由(4.18)与(4.17)有

$$\int_0^\infty y^{s-1}g(y)dy=\int_0^1 y^{s-1}g(y)dy=\frac{1}{m!s}-\sum_{n=2}^{m}\frac{(-1)^n(n-1)}{n!(m-n)!(n+s)}$$

$$=\frac{1}{s\prod\limits_{n=2}^{m}(n+s)},$$

如 $m\geqslant 2$，且 $s\neq 0,\ -2,\ -3,\ \cdots,\ -(m-1),\ -m$. 这样由Mellin变换的反转公式(参见潘承洞与潘承彪著《解析数论基础》)，可有

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{y^s ds}{s\prod\limits_{n=2}^{m}(s+n)}=g\left(\frac{1}{y}\right),\ 如\ m\geqslant 2,\ y>0. \tag{4.21}$$

因为对 $\mathrm{Re}\, s>1$，有

$$\zeta_{\mathbb{K}}(s)=\sum_{\mathfrak{A}}N(\mathfrak{A})^{-s},$$

这里 $\mathfrak{A}$ 跑过 $\mathbb{K}$的所有整理想，在(4.21)中取 $m=6$，可得

$$I\overset{\text{def}}{=}\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{\zeta_{\mathbb{K}}(s+\beta_0)x^s ds}{s\prod\limits_{n=2}^{6}(s+n)}$$

$$=\sum_{N(\mathfrak{A})<x}N(\mathfrak{A})^{-\beta_0}\left(\frac{1}{6!}-\sum_{n=2}^{6}\frac{(-1)^n(n-1)}{n!(6-n)!}\left(\frac{N(\mathfrak{A})}{x}\right)^n\right). \tag{4.22}$$

这里 $\mathfrak{A}$ 跑过 $\mathbb{K}$ 的所有其范 $\leqslant x$ 的整理想，x 为一个给定的正实数 k^A，即 $x=k^A$.

由于对每一个正整数 m，m^2 均是 $\mathbb{K}$ 中某个整理想的范，并且由(1.20)和(4.22)右边的每一项均大于等于0. 这样，由(4.22)与(4.13)可得

$$6!I\geqslant\sum_{1<m<\sqrt{x}}\frac{1}{m^2}\left(1-\sum_{n=2}^{6}(-1)^n(n-1)\binom{6}{n}\left(\frac{m^2}{x}\right)^n\right)$$

$$=\sum_{1<m<\sqrt{x}}\frac{1}{m^2}-\sum_{n=2}^{6}(-1)^n(n-1)\binom{6}{n}x^{-n}\sum_{1<m<\sqrt{x}}m^{2n-2}$$

$$>\frac{\pi^2}{6}-\frac{1}{[\sqrt{x}]}-\sum_{n=2}^{6}(-1)^n(n-1)\binom{6}{n}x^{-n}$$

$$\times\left(\frac{(\sqrt{x})^{2n-1}}{2n-1}+\theta(\sqrt{x})^{2n-2}\right), \tag{4.23}$$

其中实数 θ 满足 $|\theta|\leqslant 1$，并用到

$$\sum_{1\leqslant m\leqslant\sqrt{x}}\frac{1}{m^2}>\frac{\pi^2}{6}-\frac{1}{[\sqrt{x}]},$$

$$\sum_{1<m<\sqrt{x}}m^{2n-2}=\frac{(\sqrt{x})^{2n-1}}{2n-1}+\theta(\sqrt{x})^{2n-2},\ \text{若}\ n\geqslant 2,$$

这两者都是熟知的，可见华罗庚著《数论导引》第五章。

这样，由(4.23)可得

$$6!I>\frac{\pi^2}{6}-\frac{1}{[\sqrt{x}]}-\frac{1}{\sqrt{x}}\sum_{n=2}^{6}\frac{(-1)^n(n-1)}{2n-1}\binom{6}{n}$$

$$-\frac{1}{x}\sum_{n=2}^{6}(n-1)\binom{6}{n}$$

$$=\frac{\pi^2}{6}-\frac{1}{[\sqrt{x}]}-\frac{281}{231}\frac{1}{\sqrt{x}}-\frac{129}{x}$$

$$>\frac{\pi^2}{6}-\frac{1}{[\sqrt{x}]}\left(1+\frac{281}{231}+\frac{1}{\sqrt{x}}\right)$$

$$>\frac{\pi^2}{6}-\frac{2.512}{[\sqrt{x}]}>1.639,\ \text{如}\ A\geqslant 0.88, \tag{4.24}$$

另一方面，把(4.22)左边的积分路径移到 $\mathrm{Re}s=\alpha$，即得

$$I=\frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty}\frac{\zeta_K(s+\beta_0)x^s ds}{s\prod_{n=2}^{6}(n+s)}+\frac{L(1,\chi)x^{1-\beta_0}}{(1-\beta_0)\prod_{n=2}^{6}(n+1-\beta_0)}$$

$$+\frac{\zeta_K(\beta_0)}{6!}-\frac{\zeta_K(-2+\beta_0)x^{-2}}{2\times 4!}, \tag{4.25}$$

其中还用到(4.1)。

令 $c>0$ 是一个待定的正实数，并设 $\beta_0\geqslant\frac{3}{4}$ 为 $L(s,\chi)$ 的一个实零点，它满足

$$1-\beta_0<\frac{c}{\log k},$$

如果这样的一个实零点存在的话；否则就置

$$\beta_0=1-\frac{c}{\log k}\left(设它仍满足\ \beta_0\geqslant\frac{3}{4}\right).$$

这样做之后，易见 $\zeta_{\mathbf{K}}(\beta_0)\leqslant 0$ 与 $-\zeta_{\mathbf{K}}(2+\beta_0)<0$。再由

$$1-\beta_0\leqslant\frac{c}{\log k},$$

可得

$$x^{1-\beta_0}\leqslant e^{Ac},\quad A\left(\frac{3}{2}+\beta_0\right)\geqslant\frac{5}{2}A-\frac{Ac}{\log k}.$$

因此由(4.16)、(4.24)和(4.25)以及上述说明，可有

$$\frac{L(1,\ \chi)}{1-\beta_0}>\frac{1.639}{e^{Ac}}-\frac{0.175}{10^{6(2.5A-2)}},\ 如\ A\geqslant 0.88. \tag{4.26}$$

这样在第一种情况下，取 $A=0.92$, $c=\frac{1}{12}$，而在第二种情况下，取 $A=0.89$, $c=1$，即可由(4.26)得出引理所需的两个结论。

引理证毕。

定理 1.1 (C.L.Siegel[92])设 k 为一个正整数，χ 为 $\bmod k$ 的实原特征。则对任给的正常数 $\varepsilon>0$，均存在一个仅依赖于 ε 的正常数 $c(\varepsilon)$，使

$$L(1,\ \chi)>\frac{c(\varepsilon)}{k^{\varepsilon}}.$$

证明 见潘承彪与潘承洞著《解析数论基础》p.299.

附注 定理 1.1 中的常数 $c(\varepsilon)$，不是实效的，即不是可以有效地计算的。

定理 1.2(Tatuzawa[103]) 设正常数 ε 满足 $0<\varepsilon<\frac{1}{11.2}$，正整数 k 满足 $k>e^{\frac{1}{\varepsilon}}$。那么，除去至多可能有一个例外情况以外，对每一个 $\bmod k$ 的实原特征 χ，均有

$$L(1,\ \chi)>\frac{0.655\varepsilon}{k^{\varepsilon}}.$$

上述两个定理合称为 Siegel-Tatuzawa 定理。在本小节中，我们的主要目的是证明下面的定理：

定理 1.3 设任给的正常数 ε 满足 $0<\varepsilon\leqslant(6\log 10)^{-1}$，正整

数$k>e^{\frac{1}{\varepsilon}}$。那么,除去至多可能有一个例外情况以外,对每一个$\bmod k$的实原特征$\chi$,均有

$$L(1, \chi)>\min\left(\frac{1}{8\log k}, \frac{14\varepsilon}{k^{\varepsilon}}\right).$$

证明 令正常数ε满足$0<\varepsilon\leqslant(6\log 10)^{-1}$,再令$k_1$是使得$k_1>e^{\frac{1}{\varepsilon}}$且$\bmod k_1$的实原特征$\chi_1$满足

$$L(1, \chi_1)\leqslant(8\log k_1)^{-1}$$

的最小正整数,首先可知k_1或$-k_1$是一个基本判别式,且

$$\chi_1(*)=\left(\frac{k_1}{*}\right)\text{或}\left(\frac{-k_1}{*}\right)(\text{Kronecker 符号}).$$

由引理1.6,可知$L(s, \chi_1)$有实零点β_1,β_1满足

$$1-\beta_1<(12\log k_1)^{-1}. \tag{4.27}$$

设k是一个正整数,它满足$k>e^{\frac{1}{\varepsilon}}$。$k$或$-k$是基本判别式,$\chi$是$\bmod k$的实原特征。由上述$k_1$的取法可知,不妨设$k\geqslant k_1$。现在我们断定除去$\chi_1$可能会是例外,总有

$$L(1, \chi)>\min\left(\frac{1}{8\log k}, \frac{14\varepsilon}{k^{\varepsilon}}\right). \tag{4.28}$$

应对$k>k_1$证明(4.28)。令

$$d=\pm k, \quad d_1=\pm k_1$$

为相应的基本判别式,则有

$$\chi(*)=\left(\frac{d}{*}\right), \quad \chi_1(*)=\left(\frac{d_1}{*}\right), \tag{4.29}$$

其中这二个等式的右边均为Kronecker符号。

不难知道有且仅有以下四种可能:

(1) $d=d_0d'$, $d_1=d_0d_1'$,

其中d_0, d', d_1'均为基本判别式,且它们是两两互素的。这时$d_2=d'd_1'$也是基本判别式,注意这时也可能$d_1'=1$,但这将对证明没有妨碍;

(2) $d=-4d_0d'$, $d_1=\pm 8d_0d_1'$,

其中$-4d_0$, $\pm 8d_0$, d', d_1'均为基本判别式,且$g.c.d.(4d_0, d')=$

$g.c.d.(8d_0, d_1') = g.c.d.(d', d_1') = 1$，从而 $d_2 = \mp 8d'd_1'$ 也是基本判别式，注意此时也可能 $d_1' = 1$ 但无妨；

(3) $d = \pm 8d_0d'$, $d_1 = \mp 8d_0d_1'$,

其中 $\pm 8d_0$, d', d_1' 均为基本判别式，且 $g.c.d.(8d_0, d') = g.c.d.(8d_0, d_1') = g.c.d.(d', d_1') = 1$，从而 $d_2 = -4d'd_1'$ 也是基本判别式，注意此时也可能 $d_1' = 1$ 但无妨；

(4) $d = \pm 8d_0d'$, $d_1 = -4d_0d_1'$,

其中 $\pm 8d_0$, $-4d_0, d', d_1'$ 均为基本判别式，且有 $g.c.d.(8d_0, d') = g.c.d.(4d_0, d_1') = g.c.d.(d', d_1') = 1$，从而 $d_2 = \mp 8d'd_1'$ 也是基本判别式，注意此时也可能 $d_1' = 1$ 但无妨。

以上四种情况中，都定义了相应的基本判别式 d_2。令

$$k_2 = |d_2|, \quad \chi_2(*) = \left(\frac{d_2}{*}\right)$$

(Kronecker 符号)为 mod k_2 的实原特征，不难看到有

$$d_2 | dd_1 \ (\text{即 } k_2 | kk_1); \quad \chi_2(n) = \chi(n)\chi_1(n), \quad \text{如 } g.c.d.(n, dd_1) = 1. \tag{4.30}$$

双二次域 $F = Q(\sqrt{d}, \sqrt{d_1})$ 的 Dedekind ζ-函数

$$\zeta_F(s) = \zeta(s)L(s, \chi)L(s, \chi_1)L(s, \chi_2), \tag{4.31}$$

这可参见 L. C. Washington 著《Introduction to Cyclotomic Fields》第4.5章。命

$$\zeta_F(s) = \sum^{\infty} \frac{a_n}{n^s}, \ \mathrm{Re}s > 1. \tag{4.32}$$

用 Euler 乘积，并分别对每一个有理素数 p 进行考察，即可推知

$$a_n \geqslant 0, \ a_{n^2} \geqslant 1 \ (n = 1, 2, \cdots). \tag{4.33}$$

注意，(4.33)的推导中用到 $p \nmid dd_1$ 时，$\chi_2(p) = \chi(p)\chi_1(p)$，从而可知对任一个素数 p, $\chi(p)$, $\chi_1(p)$, $\chi_2(p)$ 不同为 -1，并可知其中有一个是零时，一定还有一个也是零。

由(4.31)及 $\zeta(s)$, $L(s, \chi)$, $L(s, \chi_1)$, $L(s, \chi_2)$ 的函数方程(参见 §1.1)，可以得到 $\zeta_F(s)$ 的函数方程：

$$\zeta_F(1-s)=\left(\frac{|d_F|}{4^{r_2}\pi^4}\right)^{s-\frac{1}{2}}\left(\frac{\Gamma\left(\frac{s}{2}\right)}{\Gamma\left(\frac{1-s}{2}\right)}\right)^{r_1}$$

$$\times\left(\frac{\Gamma(s)}{\Gamma(1-s)}\right)^{r_2}\zeta_F(s), \tag{4.34}$$

其中

$$d_F=dd_1d_2,$$

$$r_1=\begin{cases}4, \\ 0,\end{cases}\quad r_2=\begin{cases}0, & \text{如 } \chi(-1)=\chi_1(-1)=1; \\ 2, & \text{否则。}\end{cases} \tag{4.35}$$

命

$$\alpha=\frac{-3}{2}-\beta_1,\ x=|d_F|^A,\ \text{正常数 } A>0.8. \tag{4.36}$$

由函数方程(4.34)可知(t 为实数),

$$|\zeta_F(\alpha+\beta_1+it)|=\left|\zeta_F\left(-\frac{3}{2}+it\right)\right|$$

$$=\left(\frac{|d_F|}{4^{r_2}\pi^4}\right)^2\left|\frac{\Gamma\left(\frac{5}{4}-i\frac{t}{2}\right)}{\Gamma\left(-\frac{3}{4}+i\frac{t}{2}\right)}\right|^{r_1}$$

$$\times\left|\frac{\Gamma\left(\frac{5}{2}-\mathrm{i}t\right)}{\Gamma\left(-\frac{3}{2}+\mathrm{i}t\right)}\right|^{r_2}\left|\zeta_F\left(\frac{5}{2}-\mathrm{i}t\right)\right|$$

$$\leqslant\left(\frac{|d_F|}{16\pi^4}\right)^2\left|\frac{1}{2}-\mathrm{i}t\right|^4\left|\frac{3}{2}-\mathrm{i}t\right|^4\zeta\left(\frac{5}{2}\right)^4,$$

其中用到(4.35)及 Γ-函数的性质,因此由(4.10), 即有

$$|\zeta_F(\alpha+\beta_1+it)|\leqslant\left(\frac{|d_F|}{16\pi^4}\right)^2\left(\frac{1}{4}+t^2\right)^2\left(\frac{9}{4}+t^2\right)^2\left(\frac{11}{8}\right)^4. \tag{4.37}$$

由(4.36)、(4.37)可得

$$\left|\frac{9!}{2\pi\mathrm{i}}\int_{\alpha-\mathrm{i}\infty}^{\alpha+\mathrm{i}\infty}\frac{\zeta_F(s+\beta_1)x^s ds}{\prod_{n=0}^{9}(s+n)}\right|$$

$$\leqslant \frac{2835\cdot 11^4}{8192\pi^9}|d_F|^{2+A\alpha}\int_0^{\infty}\frac{\left(\frac{1}{4}+t^2\right)^2\left(\frac{9}{4}+t^2\right)^2}{\sqrt{\prod_{n=0}^{9}((\alpha+n)^2+t^2)}}dt, \tag{4.38}$$

由$\frac{3}{4}\leqslant\beta_1<1$，即知

$$\begin{aligned}\prod_{n=0}^{9}((\alpha+n)^2+t^2) &> \prod_{n=0}^{2}\left(\frac{(4n+1)^2}{16}+t^2\right)\\ &\quad\cdot\prod_{m=0}^{6}\left(\frac{(2m+1)^2}{4}+t^2\right)\\ &> \left(\frac{121}{4}+t^2\right)^2\left(\frac{1}{4}+t^2\right)^4\left(\frac{9}{4}+t^2\right)^4.\end{aligned} \tag{4.39}$$

这里用到

$$\left(\frac{25}{16}+t^2\right)\left(\frac{169}{4}+t^2\right)>\left(\frac{121}{4}+t^2\right)\left(\frac{1}{4}+t^2\right),$$

$$\left(\frac{1}{16}+t^2\right)\left(\frac{81}{4}+t^2\right)>\left(\frac{1}{4}+t^2\right)\left(\frac{9}{4}+t^2\right),$$

$$\left(\frac{81}{16}+t^2\right)\left(\frac{49}{4}+t^2\right)\left(\frac{25}{4}+t^2\right)>\left(\frac{1}{4}+t^2\right)\left(\frac{9}{4}+t^2\right)^2.$$

这样由(4.38)与(4.39)可得

$$\left|\frac{9!}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty}\frac{\zeta_F(s+\beta_1)x^s ds}{\prod_{n=0}^{9}(s+n)}\right|$$

$$<\frac{2835\cdot 11^4}{8192\pi^9}|d_F|^{2+A\alpha}\int_0^{\infty}\frac{dt}{\frac{121}{4}+t^2}$$

$$=\frac{2835\cdot 11^4}{8192\pi^9}|d_F|^{2+A\alpha}\cdot\frac{\pi}{11}<\frac{0.048545}{|d_F|^{A\left(\frac{3}{2}+\beta_1\right)-2}}, \tag{4.40}$$

其中用到(4.36)：$\alpha=-\frac{3}{2}-\beta_1$.

对正整数m，命

$$V(s)=\sum_{n=0}^{m}(-)^n\binom{m}{n}\prod_{\substack{l=0\\ l\neq n}}^{m}(s+l),$$

则 $V(s)$ 是 s 的 m 次多项式。容易证明

$$V(u)=m!,\ 如\ 0\leqslant u\leqslant m.$$

这证明了

$$\sum_{n=0}^{m}(-1)^n\binom{m}{n}\prod_{\substack{l=0\\ l\neq n}}^{m}(s+l)=m!,\ m=1,\ 2,\ \cdots$$

于是

$$\int_0^1\frac{(1-y)^m}{m!}y^{s-1}dy=\frac{1}{m!}\sum_{l=0}^{m}\frac{(-1)^l}{(s+l)}\binom{m}{l}=\frac{1}{\prod\limits_{l=0}^{m}(s+l)},$$

$$如\ m\geqslant 1,\ s\neq 0,\ -1,\ \cdots,\ -m,$$

这样，由 Mellin 变换可得(取 $m=9$)

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{y^s ds}{\prod\limits_{n=0}^{9}(n+s)}=\begin{cases}\dfrac{1}{9!}\left(1-\dfrac{1}{y}\right)^9, & 如\ y\geqslant 1;\\ 0, & 如\ 0<y\leqslant 1.\end{cases}$$

由此可得

$$I\overset{\text{def}}{=\!=}\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{\zeta_F(s+\beta_1)x^s ds}{\prod\limits_{n=0}^{9}(s+n)}$$

$$=\frac{1}{9!}\sum_{1<n<x}\frac{a_n}{n^{\beta_1}}\left(1-\frac{n}{x}\right)^9. \tag{4.41}$$

由(4.32)与(4.41)，可得

$$9!\,I\geqslant\sum_{1<n<\sqrt{x}}\frac{1}{n^2}\left(1-\frac{n^2}{x}\right)^9>\frac{\pi^2}{6}-\frac{10}{[\sqrt{x}]}>1.6447. \tag{4.42}$$

这里用到

$$x=|d_F|^A>(kk_1)^{0.8}>10^{12\times 0.8}=10^{9.6}.$$

把(4.41)左边的积分的路径移到 $\mathrm{Re}\,s=\alpha$，即有

$$I=\frac{1}{2\pi i}\int_{\alpha-i\infty}^{\alpha+i\infty}\frac{\zeta_F(s+\beta_1)x^s ds}{\prod\limits_{n=0}^{9}(n+s)}+\frac{L(1,\chi)L(1,\chi_1)L(1,\chi_2)x^{1-\beta_1}}{(1-\beta_1)\prod\limits_{n=1}^{9}(n+1-\beta_1)}$$

$$+\frac{\zeta_F(\beta_1)}{9!}-\frac{\zeta_F(-1+\beta_1)x^{-1}}{8!}+\frac{\zeta_F(-2+\beta_1)x^{-2}}{2\cdot 7!}. \tag{4.43}$$

我们有

$$\zeta_F(\beta_1)=0,\ \zeta_F(-1+\beta_1)>0, \tag{4.44}$$

前一个等式由 β_1 为 $L(s,\chi_1)$ 的一个零点及(4.31)可得,后一不等式可由函数方程(4.34)及 $\beta_1<1$ 得出。

又由函数方程(4.34)可得

$$0<\frac{9!\,\zeta_F(-2+\beta_1)\pi^{-2}}{2\cdot 7!}=36\left(\frac{|d_F|}{4^{r_2}\pi^4}\right)^{2.5-\beta_1}$$

$$\times\left(\frac{\Gamma\left(\frac{3-\beta_1}{2}\right)}{\Gamma\left(\frac{-2+\beta_1}{2}\right)}\right)^{r_1}\left(\frac{\Gamma(3-\beta_1)}{\Gamma(-2+\beta_1)}\right)^{r_2}\cdot$$

$$\zeta_F(3-\beta_1)\cdot|d_F|^{-2A}, \tag{4.45}$$

由 Γ-函数性质可得(见文献[20]p.937 的 2, 与 p.938 的 8.)

$$0<\frac{\Gamma(3-\beta_1)}{\Gamma(-2+\beta_1)}=\frac{(2-\beta_1)^2(1-\beta_1)^2}{\Gamma(\beta_1)}\ \Gamma(1-\beta_1)$$

$$=\frac{(2-\beta_1)^2(1-\beta_1)^2}{\Gamma(\beta_1)^2}\cdot\frac{\pi}{\sin(\pi\beta_1)}$$

$$=\frac{(2-\beta_1)^2\beta_1^2(1-\beta_1)}{\Gamma(1+\beta_1)^2}\cdot\frac{\pi(1-\beta_1)}{\sin(\pi(1-\beta_1))}$$

$$<\frac{(2-\beta_1)^2\beta_1^2(1-\beta_1)}{0.8856^2}\cdot\frac{\pi}{2}<\frac{225\pi}{2048\times 0.8856^2}, \tag{4.46}$$

最后一步是因为 $\frac{3}{4}\leqslant\eta<1$ 时, $(2-\eta)^2\eta^2(1-\eta)$ 在 $\eta=\frac{3}{4}$ 处达到最大值 $\frac{225}{1024}$.

令 $\beta_2=\frac{\beta_1}{2}$, 则 $\frac{3}{8}\leqslant\beta_2<\frac{1}{2}$, 且有

$$\frac{\Gamma\left(\frac{3-\beta_1}{2}\right)}{\Gamma\left(\frac{-2+\beta_1}{2}\right)}=\frac{\Gamma(1.5-\beta_2)}{\Gamma(-1+\beta_2)}=\frac{\sqrt{\pi}}{2^{2-2\beta_2}}\cdot\frac{\Gamma(3-\beta_1)}{\Gamma(2-\beta_2)}\cdot\frac{(\beta_2-1)}{\Gamma(\beta_2)}$$

$$=\frac{-\sqrt{\pi}}{2^{2-\beta_1}}\cdot\frac{(2-\beta_1)(1-\beta_1)\Gamma(1-\beta_1)}{\Gamma(1-\beta_2)\Gamma(\beta_2)}$$

$$= -\frac{\sqrt{\pi}}{2^{2-\beta_1}}\frac{(2-\beta_1)(1-\beta_1)}{\Gamma(\beta_1)}\cdot\frac{\sin\pi\beta_2}{\sin\pi\beta_1}$$

$$= -\frac{\sqrt{\pi}}{2^{2-\beta_1}}\cdot\frac{(2-\beta_1)(1-\beta_1)\beta_1}{\Gamma(1+\beta_1)}\cdot\frac{1}{2\cos\pi\beta_2}. \tag{4.47}$$

由

$$0<\frac{1-\beta_1}{\cos\pi\beta_2}=\frac{1-\beta_1}{\sin\frac{\pi(1-\beta_1)}{2}}<\frac{1}{4\sin\frac{\pi}{8}}=\frac{1}{2\sqrt{2-\sqrt{2}}},$$

$$\Gamma(1+\beta_1)>0.8856$$

及(4.47)可得

$$\left|\frac{\Gamma\left(\frac{3-\beta_1}{2}\right)}{\Gamma\left(\frac{-2+\beta_1}{2}\right)}\right|<\frac{\sqrt{\pi}\cdot 2^{\beta_1}(2-\beta_1)\beta_1}{2^4\sqrt{2-\sqrt{2}}\times 0.8856}$$

$$<\frac{\sqrt{\pi}}{7.0848\times\sqrt{2-\sqrt{2}}}, \tag{4.48}$$

注意当$\frac{3}{4}\leqslant\eta\leqslant 1$时，$2^{\eta}(2-\eta)\eta$的最大值在$\eta=1$时达到。

由(4.45)、(4.46)和(4.48)可知有：

如$r_1=4$，$r_2=0$，则

$$0<\frac{9!\,\zeta_F(-2+\beta_1)x^{-2}}{2\cdot 7!}<\frac{36}{\pi^6}\left(\frac{\sqrt{\pi}}{7.0848\sqrt{2-\sqrt{2}}}\right)^4$$

$$\times\left(\frac{\pi^2}{6}\right)^4|d_F|^{-2A+2\cdot 5-\beta_1}<0.00313|d_F|^{-2A+2\cdot 5-\beta_1};$$

如$r_1=0$，$r_2=2$，则

$$0<\frac{9!\,\zeta_F(-2+\beta_1)x^{-2}}{2\cdot 7!}<\frac{36}{(2\pi)^6}\left(\frac{225\pi}{2048\cdot 0.8856^2}\right)^2$$

$$\times\left(\frac{\pi^2}{6}\right)^4|d_F|^{-2A+2\cdot 5-\beta_1}<0.00083|d_F|^{-2A+2\cdot 5-\beta_1},$$

这样，总有

$$0<\frac{9!\,\zeta_F(-2+\beta_1)x^{-2}}{2\cdot 7!}<0.00313|d_F|^{-2A+2\cdot 5-\beta_1}. \tag{4.49}$$

取
$$A=\frac{2}{\frac{3}{2}+\beta_1},$$
则
$$0.8<A\leqslant\frac{8}{9}.$$
因此由(4.40)、(4.42)、(4.43)、(4.44)和(4.49)可得
$$1.5947(1-\beta_1)<L(1,\chi)L(1,\chi_1)L(1,\chi_2)_{3^{1-\beta_1}} \tag{4.50}$$
这里还要用到
$$\begin{aligned}0.00313|d_F|^{-2A+2.5-\beta_1}&=0.00313|d_F|^{4-2A-\frac{2}{A}}\\&\leqslant 0.00313|d_F|^{-\frac{1}{36}}\leqslant 0.00313k_1^{-\frac{1}{36}}\\&\leqslant 0.00313\cdot 10^{-\frac{1}{3}}<0.001453.\end{aligned}$$
由 §1.1及(4.31)可得：如$\sigma>1$，则有
$$\begin{aligned}\frac{\zeta_F'}{\zeta_F}(\sigma)&=\frac{\zeta'}{\zeta}(\sigma)+\frac{L'}{L}(\sigma,\chi)+\frac{L'}{L}(\sigma,\chi_1)+\frac{L'}{L}(\sigma,\chi_2)\\&=-\frac{1}{\sigma-1}+2\gamma+2\log\pi-\frac{1}{2}\log|d_F|+\sum_\rho\frac{1}{\sigma-\rho}\\&\quad-\sum_{\psi=\chi_0,\chi,\chi_1,\chi_2}\sum_{n=1}^{\infty}\frac{\sigma+\delta_\psi}{2n(\sigma+\delta_\psi+2n)},\end{aligned}\tag{4.51}$$
这里χ_0表示mod 1 的主特征，
$$\delta_\psi=\frac{1-\psi(-1)}{2},$$
ρ 跑过 $\zeta_F(s)$ 的所有非显然零点，且排列方式是将ρ与$\bar\rho$放在一起。由于$\sigma>1$时$\zeta_F'(\sigma)<0$，$\zeta_F(\sigma)>0$，即由(4.5)可知有
$$\sum_{\rho\in S}\frac{1}{\sigma-\rho}<\frac{1}{\sigma-1}+\frac{1}{2}\log|d_F|,\quad \sigma>1, \tag{4.52}$$
这里S为任一个由 $\zeta_F(s)$ 的若干实零点组成的集合，S也可能是空集。

特别取
$$\sigma=1+\frac{c}{\log|d_F|},\qquad c=2(\sqrt{2}-1),$$
则由(4.52)可知$\zeta_F(s)$至多有一个实零点β满足
$$\beta>1-\frac{2(\sqrt{2}-1)^2}{\log|d_F|}. \tag{4.53}$$

如 $L(s, \chi)$ 在区间 $\left(1-\frac{1}{12\log|d|}, 1\right)$ 中无根，则由引理1.6即知有

$$L(1, \chi)>\frac{1.51}{12}\cdot\frac{1}{\log k}>\frac{1}{8\log k},$$

由此即得所需。如果 $L(1, \chi)$ 在该区间中有根 β，则由(4.53)即知有

$$1-\beta_1\geqslant\frac{2(\sqrt{2}-1)^2}{\log|d_F|} \text{ 或 } 1-\beta\geqslant\frac{2(\sqrt{2}-1)^2}{\log|d_F|}. \tag{4.54}$$

如果(4.54)的第二个不等式成立，则由 β 的定义，应有

$$\frac{2(\sqrt{2}-1)^2}{\log|d_F|}<\frac{1}{12\log|d|},$$

由此可得

$$|d_F|>|d|^{24(\sqrt{2}-1)^2}>|d|^4,$$

又因 $d_F=dd_1d_2$，从而与(用(4.30))

$$|d_F|\leqslant|dd_1|^2<|d|^4$$

矛盾。因此必有

$$1-\beta_1\geqslant\frac{2(\sqrt{2}-1)^2}{\log|d_F|}\geqslant\frac{(\sqrt{2}-1)^2}{\log(kk_1)}. \tag{4.55}$$

命

$$M=1+[\sqrt{k_2}\log k_2], \tag{4.56}$$

由 $k_2\geqslant3$，即知 $M\geqslant2$。于是由 Polya-Vinogradov 不等式

$$\left|\sum_{x<n<y}\chi_2(n)\right|<\sqrt{k_2}\log k_2,$$

即有(并用 $k_2\leqslant kk_1$)

$$\begin{aligned}L(1, \chi_2)&<\log M+\gamma+\frac{1}{M-1}+\frac{\sqrt{k_2}\log k_2}{M+1}\\&<2+\gamma+\log(1+\sqrt{k_2}\log k_2)\\&<2+\gamma+\log(1+\sqrt{kk_1}\log(kk_1))\\&<0.72\log(kk_1)\text{，如 } kk_1\geqslant10^{12}.\end{aligned} \tag{4.57}$$

又由(4.36)有

$$x^{1-\beta_1}=|d_F|^{A(1-\beta_1)}\leqslant(kk_1)^{2A(1-\beta_1)}<(kk_1)^{\frac{0.1337}{\log k_1}},\qquad(4.58)$$

这里用到(4.27)及

$$A=\frac{2}{1.5+\beta_1},\ k_1\geqslant10^6,\ \frac{4(6\log10)}{30(6\log10)-1}$$
$$\approx0.1336\cdots<0.1337,$$

从而

$$2A(1-\beta_1)=\frac{4(1-\beta_1)}{1.5+\beta_1}=\frac{10}{1.5+\beta_1}-4<\frac{10}{2.5-\frac{1}{12\log k_1}}-4$$

$$=4\left(\frac{1}{1-\frac{1}{30\log k_1}}-1\right)$$

$$=\frac{4}{30-\frac{1}{\log k_1}}\cdot\frac{1}{\log k_1}\leqslant\frac{4(6\log10)}{30(6\log10)-1}\cdot\frac{1}{\log k_1}$$

$$<\frac{0.1337}{\log k_1}.$$

这样由(4.50)、(4.57)和(4.58)得到

$$L(1,\chi)>\frac{3.04}{\log k_1\left(1+\frac{\log k}{\log k_1}\right)^2(kk_1)^{\frac{0.1337}{\log k_1}}},\qquad(4.59)$$

这里还用到(4.55)以及由 χ_1 的定义,有

$$L(1,\chi_1)<(8\log k_1)^{-1}.$$

命

$$\eta=\frac{\log k}{\log k_1},\ \eta>1.\qquad(4.60)$$

当 $\eta\leqslant6.62$ 时,由(4.59)与(4.60)即知,有

$$L(1,\chi)>\frac{0.125}{\log k},$$

这里用到

$$\frac{3.04\eta}{(\eta+1)^2e^{0.1337(1+\eta)}}>0.125,\ \text{如}\ 1<\eta\leqslant6.62.$$

因此可设 $\eta>6.62$, 此时

$$2\log(\eta+1)<0.5331(\eta+1),$$

故有

$$L(1,\chi)>\frac{1.56}{(\log k_1)\,k^{\frac{0.6668}{\log k_1}}}. \qquad (4.61)$$

当 $0<y<0.6668\log k$ 时，$yk^{\frac{0.6668}{y}}$ 是 y 的减函数，即 $\log k_1<0.6668\log k$ 时，$(\log k_1)\,k^{\frac{0.6668}{\log k_1}}$ 是k_1的减函数。我们已设 $\frac{\log k}{\log k_1}>6.62>(0.6668)^{-1}$，故由 $\log k_1>\frac{1}{\varepsilon}$，(4.61) 即有

$$L(1,\chi)>\frac{1.56\varepsilon}{k^{0.6668\varepsilon}}=\frac{\varepsilon}{k^{\varepsilon}}(1.56k^{0.3332\varepsilon}),$$

结合

$$1.56k^{0.3332\varepsilon}=1.56e^{0.3332\varepsilon\log k}>1.56e^{0.3332\varepsilon(6.62\log k_1)}$$
$$>1.56e^{0.3332\times 6.62}>14,$$

得到

$$L(1,\chi)>\frac{14\varepsilon}{k^{\varepsilon}},$$

因此得到所要证明的。定理证毕。

附注 由 Siegel-Tatuzawa定理立即可知，当负的基本判别式 $d\to-\infty$ 时，虚二次域$K=Q(\sqrt{d})$的类数 $h_K=h(d)\to+\infty$，所以 Gauss 关于类数的第二个猜想已完全证明。

§ 2 实二次域的正则子 logε 与连分数

对一个实二次域 $K=Q(\sqrt{d})$ ($d>0$ 为判别式)，它的每一个理想类A中都有一个代表理想

$$\mathfrak{A}=\left[a,\ \frac{b+\sqrt{d}}{2}\right], \qquad (4.62)$$

其中有理整数 a, b, c 满足

$$g.c.d.(a,b,c)=1,$$
$$b^2+4ac=d,$$

$$0\leqslant|b|\leqslant a\leqslant c.$$

展开
$$\alpha_{\mathfrak{A}}=\frac{b+\sqrt{d}}{2a}$$

为简单连分数，则由第一章已知，应有

$$\alpha=\alpha_{\mathfrak{A}}=\frac{b+\sqrt{d}}{2a}=[a_0,\overline{a_1,\ \cdots,\ a_k}],\tag{4.63}$$

这里 $\overline{a_1,\ \cdots,\ a_k}$ 是基本周期，k 是基本周期的长度，记为

$$k=p(\alpha_{\mathfrak{A}}).$$

令 $\alpha_{\mathfrak{A}}$ 的第 n 个完全商为

$$\alpha_n=[a_n,\ a_{n+1},\ \cdots]=\frac{P_n+\sqrt{d}}{2Q_n}\ (n\geqslant 0),\tag{4.64}$$

则有理整数 P_n, Q_n …满足

$$P_{n+1}+P_n=2a_nQ_n(n\geqslant 0),\ P_{n+1}^2+4Q_nQ_{n+1}=d(n\geqslant 0),\tag{4.65}$$

$$1\leqslant Q_n<\sqrt{d}\ (n\geqslant 0),\ \ |\sqrt{d}-2Q_n|<P_n<\sqrt{d}\ (n\geqslant 1).\tag{4.66}$$

再令 $\alpha=\alpha_{\mathfrak{A}}$ 的第 n 个渐近分数为

$$\frac{p_n}{q_n}=[a_0,\ a_1,\ \cdots,\ a_n]\ (n\geqslant 0).\tag{4.67}$$

则 K 的基本单位

$$\varepsilon=p_{k-1}+\frac{\sqrt{d}-b}{2a}q_{k-1}.\tag{4.68}$$

A 中的任一个整理想 $\hat{\mathfrak{A}}$ 都具有下列形状：

$$\hat{\mathfrak{A}}=\hat{c}\left[\hat{a},\ \frac{\hat{b}+\sqrt{d}}{2}\right],$$

其中有理数 $\hat{a}$, $\hat{b}$, $\hat{c}$ 满足 $\hat{a}\geqslant 1$, $\hat{c}\geqslant 0$, $4\hat{a}|d-\hat{b}^2$。因为

$$\alpha_{\hat{\mathfrak{A}}}=\frac{\hat{b}+\sqrt{d}}{2\hat{a}}$$

相似于

$$\alpha_{\mathfrak{A}}=\frac{b+\sqrt{d}}{2a}$$

(这可很容易地由相应二次型的广义相似得出。设 $\delta=\pm 1$, 使

$$((\delta\hat{a},\ \delta\hat{b},\ \delta c_1))\underset{\smile}{\begin{pmatrix}\mathrm{rs}\\ \mathrm{tu}\end{pmatrix}}((a,\ \delta b,\ -c)),$$

则

$$\frac{\hat{b}+\sqrt{d}}{2\hat{a}}=\begin{pmatrix}\delta u & t\\ \delta s & r\end{pmatrix}\left\langle\frac{b+\sqrt{d}}{2a}\right\rangle,$$

所以 $\alpha_{\hat{\mathfrak{A}}}$ 的简单连分数展开式的基本周期的长度与 $\alpha_{\mathfrak{A}}$ 的是相等的。这个为类 A 所共有的长度 k，我们称为 A 的长度，并记为

$$k=p(A)。\tag{4.69}$$

本节中我们要证明的基本结果是定理 2.1。

定理 2.1 对任一个实二次域 $K=Q(\sqrt{d})$ ($d>0$ 为判别式)，存在两个与 d 无关的正常数 c_1, c_2, 使

$$c_1<\frac{\sum\limits_{A\in\mathscr{C}_K}p(A)}{h_K\log\varepsilon}<c_2,$$

其中 $\mathscr{C}_K$ 为 K 的理想类群，h_K 为 $\mathscr{C}_K$ 的阶，ε 为 K 的基本单位，$p(A)$ 为 A 的长度，定义如上。正常数 c_2 是可以有效地计算的，即它是实效的，但正常数 c_1 是非实效的，即它不是可以有效地计算的，同时除去可能有一个实二次域是例外，c_1 可以是实效的。

附注 令

$$p(K)=\frac{1}{h_K}\sum_{A\in\mathscr{C}_K}p(A),$$

并称它为 K 的长度，即它是理想类的平均长度，则定理 2.1 可改写为

$$c_1<\frac{p(K)}{\log\varepsilon}<c_2,$$

这里 c_1, c_2 是与 K 无关的正常数。所以域 K 的长度是与域 K 的正则子 $\log\varepsilon$ 具有相同的无穷大阶。

定理 2.1 的证明

对 $d\leqslant 2^{64}$ 的域，定理显然成立，故可设 $d>2^{64}$。

实效正常数 c_2 的存在是很明显的。由 (4.68) 即有

$$\varepsilon\geqslant\left(\frac{1+\sqrt{5}}{2}\right)^k,$$

所以由定义 (4.69) 有

$$p(A)=k\leqslant c_2\log\varepsilon,$$

$$c_2=\frac{1}{\log\frac{1+\sqrt{5}}{2}}\approx 2.078\cdots$$

这样得到了定理中的第二个不等式，而定理中的第一个不等式的证明，就没有这么简单了。

我们首先来证明下列等式

$$\sum_{A\in\mathscr{C}_K} p(A)=\sum_{\substack{1<x<\sqrt{d}\\ |\sqrt{d}-2x|<y<\sqrt{d}\\ y^2\equiv d(\bmod 4x)}} 1 \tag{4.70}$$

事实上，对每一个 $A\in\mathscr{C}_K$ 我们取 A 的如(4.62) 所述的代表理想 $\mathfrak{A}$，则 $p(A)=p(\alpha_{\mathfrak{A}})$，$p(\alpha_{\mathfrak{A}})$ 即为 $\alpha_{\mathfrak{A}}$ 的 k 个完全商

$$\alpha_n=\frac{P_n+\sqrt{d}}{2Q_n}\quad(1\leqslant n\leqslant k)$$

的个数。由(4.65)与(4.66)即知这些$\frac{P_n+\sqrt{d}}{2Q_n}$均作为(4.70)右边的某个$\frac{Y+\sqrt{d}}{2X}$出现。反之，对右边定义出的一个 $\frac{Y+\sqrt{d}}{2X}$，命 $Q=X$，$P=2X+Y$，则 $\omega=\frac{P+\sqrt{d}}{2Q}$ 是约化的，即有

$$0<\omega'<1<\omega,$$

且有 $Q\left|\frac{P^2-d}{4}\right.$，其实易见还有

$$\omega=\frac{2X+Y+\sqrt{d}}{2X}>2. \tag{4.71}$$

这样，由第一章的引理 1.9 即知，存在某个 $A\in\mathscr{C}_K$，以及 A 的一个如(4.62)所述的代表理想 $\mathfrak{A}=\left[a,\frac{b+\sqrt{d}}{2}\right]$，使

$$P=2Q_{n+1}-P_{n+1}+2(P_{n+1}+Q_n)t-2Q_nt^2, \tag{4.72}$$

$$Q=Q_{n+1}+tP_{n+1}-t^2Q_n, \tag{4.73}$$

$$1\leqslant t\leqslant a_n,\ 1\leqslant n\leqslant k. \tag{4.74}$$

因此由定义及(4.72)、(4.73)有

$$X=Q_{n+1}+tP_{n+1}-t^2Q_n,\ Y=2Q_nt-P_{n+1}. \tag{4.75}$$

由(4.71)与(4.75)可得

$$1<\frac{Y+\sqrt{d}}{2X}=\frac{2Q_nt-P_{n+1}+\sqrt{d}}{2(Q_{n+1}+tP_{n+1}-t^2Q_n)}$$

$$=\frac{2Q_n}{\sqrt{d}+P_{n+1}-2Q_nt},\tag{4.76}$$

最后一步还用了(4.65)．由(4.76)有

$$1>\frac{\sqrt{d}+P_{n+1}-2Q_nt}{2Q_n}=a_n-t+\frac{\sqrt{d}-P_n}{2Q_n},\tag{4.77}$$

其中也用了(4.65)。由(4.74)、(4.66)有

$$1\leqslant t\leqslant a_n,\ 0<\frac{\sqrt{d}-P_n}{2Q_n}<1,$$

由此及(4.77)即得出

$$t=a_n.\tag{4.78}$$

由(4.78)、(4.75)和(4.65)即有

$$X=Q_{n-1},\ Y=P_n,\ 1\leqslant n\leqslant k.$$

由此及第一章的引理 1.5 即知，$\frac{Y+\sqrt{d}}{2X}$ 是 A^{-1} 的代表理想的某个完全商。显然完全商与$\frac{Y+\sqrt{d}}{2X}$的这种对应关系是双方一一的。综上述，我们证明了(4.70)。

下面由(4.70)出发来证明我们的定理。由(4.70)可得

$$\sum_{A\in\mathscr{F}_K}p(A)\geqslant\sum_{1<x<\frac{\sqrt{d}}{2}}\ \sum_{\substack{\sqrt{d}-2x<y<\sqrt{d}\\ y^2\equiv d(\bmod 4x)}}1$$

$$=\frac{1}{2}\sum_{1<n<\frac{\sqrt{d}}{2}}f_d(4n),\tag{4.79}$$

其中 $f_d(4n)$是同余方程

$$x^2\equiv d(\bmod 4n)$$

$x \bmod 4n$ 的解数。由第一章的引理 2.13 即知

$$f_d(4n)=\prod_{p^m\|4n}f_d(p^m),\tag{4.80}$$

这里 p 表有理素数，$f_d(1)=1$，以及

(1) 如奇素数 $p\nmid d$，则 $\left(\chi_d(*)=\left(\frac{d}{*}\right)\text{为 Kronecker 符号}\right)$

$$f_d(p^m)=1+\chi_d(p),\ m\geqslant 1;$$

(2) 如奇素数 $p|d$, 则

$$f_d(p)=1;\ f_d(p^m)=0,\ \text{如 } m\geqslant 2;$$

(3) 如 d 奇, 即 $d\equiv 1(\bmod 4)$时, 则

$$f_d(2^2)=2;$$

$$f_d(2^{m+2})=4,\ \text{如 } m\geqslant 1 \text{ 且 } d\equiv 1(\bmod 8);$$

$$f_d(2^{m+2})=0,\ \text{如 } m\geqslant 1 \text{ 且 } d\equiv 5(\bmod 8);$$

(4) 如 d 偶, 即 $4|d$, 而 $\frac{d}{4}\equiv 2$ 或 $3(\bmod 4)$, 则

$$f_d(2^2)=f_d(2^3)=2;\ f_d(2^m)=0,\ \text{如 } m\geqslant 4.$$

这样, 命

$$g(n)=\frac{1}{2}f_d(4n),\ n\geqslant 1. \tag{4.81}$$

则由上述可知

$$g(n)\geqslant 0, \tag{4.82}$$

且有

$$G(s)\overset{\text{def}}{=\!=}\sum_{n=1}^{\infty}\frac{g(n)}{n^s}=\frac{\zeta(s)}{\zeta(2s)}L(s,\chi_d),\ \operatorname{Re}s>1. \tag{4.83}$$

$G(s)$ 可以解析开拓至整个 s 平面, 而成为一个半纯函数, 并在 $\operatorname{Re}s\geqslant\frac{1}{2}$ 中除去 $s=1$ 这个一阶极点外是解析的, $G(s)$在 $s=1$处的残数为$\frac{6}{\pi^2}L(1,\chi_d)$, $\chi_d(*)=\left(\frac{d}{*}\right)$是 Kronecker 符号,

$$G\left(\frac{1}{2}\right)=0.$$

这样由(4.79)与(4.81)即得

$$\sum_{A\in\mathscr{F}_K}p(A)\geqslant\sum_{1<n<\frac{\sqrt{d}}{2}}g(n). \tag{4.84}$$

令 $\eta(n)=|\mu(n)|$, μ 为 μöbius 函数。则有

$$\frac{\zeta(s)}{\zeta(2s)}=\sum_{n=1}^{\infty}\frac{\eta(n)}{n^s},\ \operatorname{Re}s>1. \tag{4.85}$$

于是由(4.83)与(4.85), 对任一个实数 $X>1$ 有

$$\sum_{1<n<X}\left(1-\frac{n}{X}\right)g(n)=\sum_{1<n<X}\left(1-\frac{n}{X}\right)\sum_{1<m|n}\chi_d(m)\eta\left(\frac{n}{m}\right)$$
$$=\sum_{1<m<X}\chi_d(m)\sum_{1<n<\frac{X}{m}}\left(1-\frac{mn}{X}\right)\eta(n)$$
$$=\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{X^s}{s(s+1)}\cdot\frac{\zeta(s)}{\zeta(2s)}\left(\sum_{1<m<X}\frac{\chi_d(m)}{m^s}\right)ds$$
$$=\frac{3X}{\pi^2}\sum_{1<m<X}\frac{\chi_d(m)}{m}+\frac{1}{2\pi i}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\frac{X^s}{s(s+1)}$$
$$\times\frac{G(s)}{L(s,\chi_d)}\left(\sum_{1<m<X}\frac{\chi_d(m)}{m^s}\right)ds, \tag{4.86}$$

熟知,我们有

$$\zeta\left(\frac{1}{2}+it\right)\ll\hat{t}^{\frac{1}{6}}\log\hat{t},\ \hat{t}=\max\{8\pi,\ |t|\}, \tag{4.87}$$

其中"≪"所含正常数为一个可以有效计算的绝对正常数。

我们来证明

$$|\zeta(1+it)|>\frac{3}{8},\ 如|t|\leqslant 2, \tag{4.88}$$

$t=0$ 时,(4.88)显然,故可设 $t\neq 0$, 且不妨只考虑 $t>0$。由 Euler 求和可知有

$$\zeta(s)=\frac{1}{2}+\frac{1}{s-1}+\frac{s}{12}-s(s+1)$$
$$\times\int_1^\infty\frac{\frac{1}{2}\{u\}^2-\frac{1}{2}\{u\}+\frac{1}{12}}{u^{s+2}}du,\ s=\sigma+it,\ \sigma\geqslant 1,\ s\neq 1,$$

由此即有

$$|\zeta(1+it)|\geqslant\left|\frac{1}{2}+\frac{1}{it}+\frac{1+it}{12}\right|-\frac{|1+it|\cdot|2+it|}{12}\int_1^\infty\frac{du}{u^3}$$
$$=\frac{\left|7+i\left(t-\frac{12}{t}\right)\right|}{12}-\frac{|(1+it)(2+it)|}{24}$$
$$=\frac{1}{24}\left(2\sqrt{49+\left(\frac{12}{t}-t\right)^2}-\sqrt{(1+t^2)(4+t^2)}\right)$$

$$\geqslant \frac{2-\sqrt{\frac{8}{13}}}{24}\sqrt{49+\left(\frac{12}{t}-t\right)^2}, \tag{4.89}$$

这是因为 $0<t\leqslant 2$ 时,

$$\frac{49+\left(\frac{12}{t}-t\right)^2}{(1+t^2)(4+t^2)}$$

是 t 的减函数,它于 $t=2$ 时达到极小值 $=\frac{13}{8}$。

又 $0<t\leqslant 2$ 时, $49+\left(\frac{12}{t}-t\right)^2$ 也是 t 的减函数, 它于 $t=2$ 时达到极小值 65, 由此及(4.89)即知(4.88)成立。

又已知有

$$\zeta(1+it)^{-1}\ll \log|t|, \text{ 如 } |t|\geqslant 2, \tag{4.90}$$

其中"≪"所含正常数为可以有效计算的绝对正常数。

(4.87) 与(4.90) 可见之于潘承洞与潘承彪著《解析数论基础》。

设 η 为一个任意给定的正常数,设它满足

$$0<\eta\leqslant\frac{1}{8}.$$

再设实数 X 满足 $d^{\frac{3}{8}+\eta}\leqslant X\leqslant d^{\frac{1}{2}}$. 令

$$\delta=\frac{\eta}{4\eta+1.5}. \tag{4.91}$$

对 $\mathrm{Re}s=\frac{1}{2}$, 有

$$\sum_{1<n<X}\frac{\chi_d(n)}{n^s}=1+\sum_{l=1}^{L}\sum_{2^{l-1}<u<2^l}\chi_d(u)u^{-it}u^{-\frac{1}{2}} + \sum_{2^L<u<X}\chi_d(u)u^{-it-\frac{1}{2}}, \tag{4.92}$$

其中

$$L=\left[\frac{\log X}{\log 2}\right]. \tag{4.93}$$

因此,用分部求和,由(4.92)即有

$$\sum_{1<n<X}\frac{\chi_d(n)}{n^s}\ll 1+\sum_{l=1}^{L+1}M(2^{l-1})2^{-\frac{l}{2}},\quad s=\frac{1}{2}+it. \tag{4.94}$$

这里，对任一个正整数 N，定义

$$M(N)=\max_{1<M<N}\Big|\sum_{M<n<2M}\chi_d(n)n^{-it}\Big|. \tag{4.95}$$

Heath-Brown[27] 证明了

$$M(N)\ll N^{\frac{1}{2}}(dT)^{\frac{3}{16}}(\tau(d))^{\frac{3}{4}}(\log(dT))^{\frac{3}{8}},$$

$$\text{如}\quad N\ll d^{\frac{5}{8}}T^{\frac{1}{8}}(\tau(d))^{-\frac{3}{2}}(\log(dT))^{-\frac{1}{4}}, \tag{4.96}$$

其中 $T=|t|+2$，$\tau(d)$是 d 的正因子个数，"$\ll$"所含的正常数是可有效计算的绝对正常数。

这样，由(4.93)—(4.96)可得

$$\sum_{1<n<X}\frac{\chi_d(n)}{n^s}\ll(dT)^{\frac{3}{16}+\frac{\eta}{4}},\quad s=\frac{1}{2}+it, \tag{4.97}$$

"$\ll$"所含的正常数仅与 η 有关，且可有效地计算。

Burgess[8]证明了，如 η 如上给定，则对任意的正整数N和H，故有

$$\sum_{N+1<n<N+H}\chi_d(n)\ll H^{\frac{1}{2}}d^{\frac{3}{16}+\frac{\eta}{4}}, \tag{4.98}$$

"$\ll$"所含正常数仅与 η 有关，且可有效地计算。

由(4.98)可得

$$\begin{aligned}\sum_{1<n<X}\frac{\chi_d(n)}{n}&=L(1,\ \chi_d)-\sum_{n>X}\frac{\chi_d(n)}{n}\\&=L(1,\ \chi_d)-\sum_{l=1}^{\infty}\sum_{2^{l-1}X<n<2^lX}\frac{\chi_d(n)}{n}\\&=L(1,\ \chi_d)+O\Big(\sum_{l=1}^{\infty}\max_{1<H<2^{l-1}X}\\&\qquad\times\Big|\sum_{2^{l-1}X<n<2^{l-1}X+H}\chi_d(n)\Big|\cdot\frac{1}{2^{l-1}X}\Big)\\&=L(1,\ \chi_d)+O\Big(\frac{d^{\frac{3}{16}+\frac{\eta}{4}}}{\sqrt{X}}\Big),\end{aligned} \tag{4.99}$$

O 所含正常数仅与 η 有关，且可以有效地计算。

这样，由(4.86)、(4.87)、(4.88)、(4.90)、(4.97)和(4.99)，即知有

$$\sum_{1<n<X}\Big(1-\frac{n}{X}\Big)g(n)-\frac{3X}{\pi^2}L(1,\ \chi_d)$$

$$\ll X^{\frac{1}{2}}d^{\frac{3}{16}+\frac{\eta}{4}}+X^{\frac{1}{2}}d^{\frac{3}{16}+\frac{\eta}{4}}\int_0^{\infty}\frac{(t+2)^{\frac{1}{6}+\frac{3}{16}+\frac{\eta}{4}}(\log(t+2))^2}{\frac{1}{4}+t^2}dt, \tag{4.100}$$

“$\ll$”所含正常数仅与 η 有关，且可以有效地计算。

由于
$$\frac{1}{6}+\frac{3}{16}+\frac{\eta}{4}<1,$$
故(4.100)右边的积分收敛。从而由(4.100)即知，当
$$d^{\frac{3}{8}+\eta}\leqslant X\leqslant d^{\frac{1}{2}},\quad 0<\eta\leqslant\frac{1}{8}$$
时，有
$$\sum_{1<n<X}\left(1-\frac{n}{X}\right)g(n)=\frac{3X}{\pi^2}L(1,\ \chi_d)+O(X^{1-\delta}), \tag{4.101}$$
O 所含正常数仅与 δ 有关，且可有效地计算，δ 由(4.91)给出。

(4.101)成立的范围是
$$0<\delta\leqslant\frac{1}{16},\quad d^{\frac{3}{8(1-4\delta)}}\leqslant X\leqslant d^{\frac{1}{2}}. \tag{4.102}$$

对任一个实数 $X>1$，命
$$\hat{G}(X)=\sum_{1<n<X}g(n), \tag{4.103}$$
则有
$$\hat{G}_1(X)\overset{\text{def}}{=\!=}\int_1^X\hat{G}(\xi)d\xi=\sum_{1<n<X}(X-n)g(n). \tag{4.104}$$

由(4.82)有 $g(n)\geqslant 0$，故可知对任给的满足
$$0<\rho\leqslant\frac{1}{2}$$
的正数 ρ，有
$$\frac{1}{\rho X}\int_{(1-\rho)X}^{X}\hat{G}(\xi)d\xi\leqslant\hat{G}(X)\leqslant\frac{1}{\rho X}\int_X^{(1+\rho)X}\hat{G}(\xi)d\xi. \tag{4.105}$$

令 X 满足
$$2d^{\frac{3}{8}+\eta}\leqslant X\leqslant\frac{2}{3}d^{\frac{1}{2}}, \tag{4.106}$$

并取

$$\rho=\frac{1}{2}X^{-\frac{\delta}{2}}\leqslant\frac{1}{2}. \tag{4.107}$$

那么由(4.101)—(4.104)与(4.106)—(4.107)，即有

$$\frac{1}{\rho X}\int_{(1-\rho)X}^{X}\hat{G}(\xi)d\xi=\frac{1}{\rho X}(\hat{G}_1(X)-\hat{G}_1((1-\rho)X))$$

$$=\frac{1}{\rho X}\left(\frac{3}{\pi^2}L(1,\chi_d)(X^2-(1-\rho)^2X^2)+O(X^{2-\delta})\right)$$

$$=\frac{6}{\pi^2}L(1,\chi_d)X+O(L(1,\chi_d)\rho X)+O\left(\frac{X^{1-\delta}}{\rho}\right)$$

$$=\frac{6}{\pi^2}L(1,\chi_d)X+O(X^{1-\eta_1}),$$

$$\eta_1=\frac{\delta}{3}=\frac{\eta}{12\eta+4.5}, \tag{4.108}$$

O 所含正常数仅与 η 有关，且可效地计算。

同理可知有

$$\frac{1}{\rho X}\int_{X}^{(1+\rho)X}\hat{G}(\xi)d\xi=\frac{6}{\pi^2}L(1,\chi_d)X+O(X^{1-\eta_1}),$$

$$\eta_1=\frac{\delta}{3}=\frac{\eta}{12\eta+4.5}, \tag{4.109}$$

O 所含正常数仅与 η 有关，且可有效地计算。

这样，由(4.103)、(4.105)、(4.108)与(4.109)即得：

对任一个满足 $0<\eta\leqslant\frac{1}{8}$ 的正常数 η，如实数 X 满足

$$2d^{\frac{3}{8}+\eta}\leqslant X\leqslant\frac{2}{3}d^{\frac{1}{2}},$$

则有

$$\sum_{1<n<X}g(n)=\frac{6}{\pi^2}L(1,\chi_d)X+O(X^{1-\eta_1}),$$

$$\eta_1=\frac{\eta}{12\eta+4.5}, \tag{4.110}$$

O 所含正常数仅与 η 有关，且可有效地计算。

由(4.84)与(4.110)得知，当 $d\geqslant2^{64}$ 时，对 $0<\eta\leqslant\frac{3}{32}$，有

$$\sum_{A\in\mathscr{P}_K} p(A) \geqslant \frac{3}{\pi^2} L(1, \chi_d)\sqrt{d} + O(d^{\frac{1}{2}-\eta_2}),$$

$$\eta_2 = \frac{\eta}{24\eta+9}, \tag{4.111}$$

O 所含正常数仅与 η 有关，且可有效地计算。

由定理 1.1—定理 1.3(Siegel-Tatuzawa 定理)及(4.111) 即知，

$$\sum_{A\in\mathscr{P}_K} p(A) \geqslant 2c_1 L(1, \chi_d)\sqrt{d},$$

这里 c_1 为一个与 d 无关的正常数(当然是非实效，并且除去可能有一个实二次域例外，c_1 可以是实效的)，再由类数公式即得

$$\sum_{A\in\mathscr{P}_K} p(A) \geqslant c_1 h_K \log\varepsilon.$$

定理证毕。

§3　二次 Euclid 域

本节中我们介绍二次 Euclid 域。在有理整数环中有 Euclid 算法，这在古代的中国、希腊和罗马时代是早已知道的。在 Gauss 研究二次域时，也明确了一些二次域的代数整数环是有 Euclid 算法的，这种其代数整数环有Euclid算法的代数数域称为 Euclid域。Euclid 域的类数当然是 1，所以首先的任务就是找出所有的二次 Euclid 域。虚二次的 Euclid 域早已阐明，即有以下定理：

定理 3.1　有且仅有 5 个虚二次 Euclid 域：

$Q(\sqrt{-3})$, $Q(\sqrt{-4})$, $Q(\sqrt{-8})$, $Q(\sqrt{-7})$, $Q(\sqrt{-11})$。

证明　见华罗庚著《数论导引》p.500。

关于实二次 Euclid 域的确定，是比较晚才解决的，数学大师华罗庚等对此均有贡献。最后解决应归功于Davenport[12]。因此，有下面的定理 3.2。

定理 3.2 (Davenport)　有且仅有 16 个实二次 Euclid 域：

$Q(\sqrt{d})$, $d=5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 57, 73, 76$。

3.1 Davenport 定理的证明(一)

本小节中我们来证明定理 3.2 中列举的 16 个实二次域均是 Euclid 域。

对正的基本判别式 d，命

$$f_d(x, y)=\begin{cases} x^2+xy-\dfrac{d-1}{4}y^2, & \text{如 } d\equiv 1 \pmod 4; \\ x^2-\dfrac{d}{4}y^2, & \text{如 } d\equiv 0 \pmod 4. \end{cases}$$

则容易验证：$K=Q(\sqrt{d})$ 为 Euclid 域的充要条件是对任给的有理数对 h、k，均存在有理整数 x、y，使

$$|f_d(x+h,\ y+k)|<1,$$

并且如有理整系数二元二次型 $F(X,\ Y)=aX^2+bXY+cY^2$ 相似于 $\pm f_d(x,\ y)$，则上述 f_d 也可换为 F。

首先不妨设上述判别准则中的 k 满足 $0\leqslant k<\dfrac{1}{2}$。

(1) 考虑 $F=x^2+bxy+cy^2$，而判别式 $d=b^2-4c$ 满足

$$0\leqslant dk^2<5 \tag{4.112}$$

时，特别当 $d=5,\ 8,\ 12,\ 13,\ 17$ 时，条件(4.112)成立。这时，取 $N\in\mathbb{Z}$，使

$$-\frac{1}{2}\sqrt{dk^2+4}<h+\frac{b}{2}k+N\leqslant-\frac{1}{2}\sqrt{dk^2+4}+1, \tag{4.113}$$

则有

$$F(h+N,\ k)=\left(h+N+\frac{b}{2}k\right)^2-\frac{d}{4}k^2. \tag{4.114}$$

由(4.112)—(4.114)，即有

$$-1<F(h+N,\ k)<1.$$

这就证明 $d=5,\ 8,\ 12,\ 13,\ 17$ 时，$Q(\sqrt{d})$ 是 Euclid 域。

(2) 考虑 $F=x^2+bxy+cy^2$，而判别式 $d=b^2-4c$ 满足

$$0\leqslant dk^2<8 \tag{4.115}$$

时，特别当 $d=21,\ 24,\ 28,\ 29$ 时，条件(4.115)成立。(1) 中已考

虑过 $dk^2<5$ 成立的情况，又 $dk^2=5$ 显然不可能，故可设

$$5<dk^2<8. \tag{4.116}$$

这时，取 $N\in\mathbb{Z}$，有

$$-\frac{1}{2}\sqrt{dk^2+4}+2<h+N+\frac{b}{2}k\leqslant-\frac{1}{2}\sqrt{dk^2+4}+3. \tag{4.117}$$

在(4.117)成立，且(4.116)也成立的情况下，容易验证下式成立。

$$-\frac{1}{2}\sqrt{dk^2+4}+2<\frac{1}{2}\sqrt{dk^2-4}<-\frac{1}{2}\sqrt{dk^2-4}+2$$
$$<-\frac{1}{2}\sqrt{dk^2+4}+3<\frac{1}{2}\sqrt{dk^2+4}.$$

因此，(4.117)必为下列两种情况之一

$(2)_1$: $-\frac{1}{2}\sqrt{dk^2+4}+2<h+N+\frac{b}{2}k<-\frac{1}{2}\sqrt{dk^2-4}+2$;

$(2)_2$: $\frac{1}{2}\sqrt{dk^2-4}<h+N+\frac{b}{2}k<\frac{1}{2}\sqrt{dk^2+4}$.

在$(2)_1$成立时，$|F(h-2+N,\ k)|<1$;

在$(2)_2$成立时，$|F(h+N,\ k)|<1$.

因此 $d=21,\ 24,\ 28,\ 29$ 时，$Q(\sqrt{d})$是 Euclid 域。

(3) $d=37$，$F=x^2+5xy-3y^2$。由(1)，(2)知道，可设 $dk^2\geqslant 8$。又 $dk^2=8$ 是不可能的，故可设

$$dk^2>8,\ 即\ 37k^2>8. \tag{4.118}$$

取 $N\in\mathbb{Z}$，使

$$-\frac{1}{2}\sqrt{dk^2+4}+\frac{5}{2}<h+N+\frac{b}{2}k\leqslant-\frac{1}{2}\sqrt{dk^2+4}+\frac{7}{2}. \tag{4.119}$$

分几种子情况分别考虑之。

$(3)_1$ 当下列条件成立时:

$$8<37k^2<\frac{33}{4}, \tag{4.120}$$

这时有

$$0<-\frac{1}{2}\sqrt{dk^2+4}+\frac{5}{2}<\frac{1}{2}\sqrt{dk^2-4}<\frac{1}{2}\sqrt{dk^2+4}$$

$$< -\frac{1}{2}\sqrt{dk^2+4}+\frac{7}{2}.$$

因此又有下列三种不同的情况。

$(3)_{11}$ 如有

$$-\frac{1}{2}\sqrt{dk^2+4}+\frac{5}{2}<h+N+\frac{b}{2}k\leqslant\frac{1}{2}\sqrt{dk^2-4},$$

则有

$$|F(h+N,\ k-1)| = \left|\left(h+N+\frac{b}{2}k-\frac{5}{2}\right)^2 - \frac{37}{4}(k-1)^2\right|<1;$$

$(3)_{12}$ 如有

$$\frac{1}{2}\sqrt{dk^2-4}<h+N+\frac{b}{2}k<\frac{1}{2}\sqrt{dk^2+4},$$

则有

$$|F(h+N,\ k)| = \left|\left(h+N+\frac{b}{2}k\right)^2-\frac{d}{4}k^2\right|<1;$$

$(3)_{13}$ 如有

$$\frac{1}{2}\sqrt{dk^2+4}\leqslant h+N+\frac{b}{2}k\leqslant -\frac{1}{2}\sqrt{dk^2+4}+\frac{7}{2},$$

则有

$$0<F(h+N-1,\ k-1)<1.$$

$(3)_2$ 当下列条件成立时：

$$\frac{33}{4}<37k^2,$$

$\left(\text{注意：}\frac{33}{4}=37\,k^2\text{ 是不可能的}\right)$这时有

$$0<-\frac{1}{2}\sqrt{dk^2+4}+\frac{5}{2}<\frac{1}{2}\sqrt{dk^2-4}<-\frac{1}{2}\sqrt{dk^2-4}+\frac{5}{2}$$

$$<-\frac{1}{2}\sqrt{dk^2+4}+\frac{7}{2}<\frac{1}{2}\sqrt{dk^2+4}.$$

因此又有下列二种不同的情况：

$(3)_{21}$ 如有

$$\frac{1}{2}\sqrt{dk^2-4}<h+N+\frac{b}{2}k<\frac{1}{2}\sqrt{dk^2+4},$$

则有

$$|F(h+N,\ k)|<1;$$

$(3)_{22}$ 如有

$$-\frac{1}{2}\sqrt{dk^2+4}+\frac{5}{2}<h+N+\frac{b}{2}k\leqslant\frac{1}{2}\sqrt{dk^2-4},$$

则有

$$|F(h+N,\ k-1)|<1.$$

因此 $Q(\sqrt{37})$是 Euclid 域。

(4) $F=2x^2+bxy+cy^2$，而判别式 $d=b^2-8c$ 满足条件

$$0\leqslant dk^2<12 \tag{4.121}$$

时，特别 $d=33,\ 41,\ 44$ 时条件 (4.121) 成立(注意 $f_{33}(3,\ -1)=-2,\ f_{41}(3,\ 1)=2,\ f_{44}(3,\ 1)=-2$)。这时取 $N\in\mathbb{Z}$，使

$$-\frac{1}{4}\sqrt{dk^2+8}<h+N+\frac{b}{4}k\leqslant-\frac{1}{4}\sqrt{dk^2+8}+1.$$

我们区分为几种情况分别考虑之。

$(4)_1$ 当 $dk^2<8$ 时，分别讨论

$$-\frac{1}{4}\sqrt{dk^2+8}<h+N+\frac{b}{4}k\leqslant0 \quad 和$$

$$0<h+N+\frac{b}{4}k\leqslant-\frac{1}{4}\sqrt{dk^2+8}+1.$$

这二种不同的情形，均可证明

$$|F(h+N,\ k)|<1;$$

$(4)_2$ 当 $8<dk^2<12$ 成立时(注意：$dk^2=8$ 不可能成立)，容易验证有：

$$-\frac{1}{4}\sqrt{dk^2+8}<\frac{1}{4}\sqrt{dk^2-8}-1<-\frac{1}{4}\sqrt{dk^2+8}+1$$
$$<\frac{1}{4}\sqrt{dk^2+8}-1.$$

因此又可区分为下列二种不同的情形：

$(4)_{21}$ 如有

$$-\frac{1}{4}\sqrt{dk^2+8}<h+N+\frac{b}{4}k\leqslant\frac{1}{4}\sqrt{dk^2-8}-1,$$

则有

$$|F(h+N,\ k)|<1;$$

$(4)_{22}$ 如有

$$\frac{1}{4}\sqrt{dk^2-8}-1<h+N+\frac{b}{4}k<\frac{1}{4}\sqrt{dk^2+8}-1,$$

则有

$$|F(h+N+1,\ k)|<1.$$

所以证明了当 $d=33,\ 41,\ 44$ 时，$Q(\sqrt{d})$是 Euclid 域。

(5) $d=57$，$F=2x^2+5xy-4y^2$ 时(注意 $f_{57}(5,\ -1)=-2$)，由(4)知，可设 $dk^2>12$($dk^2=12$ 显然不可能)。取 $N\in\mathbb{Z}$，使

$$-\frac{1}{4}\sqrt{dk^2+8}+\frac{5}{4}<h+N+\frac{5}{4}k\leqslant-\frac{1}{4}\sqrt{dk^2+8}+\frac{9}{4}.$$

区分为几种情况讨论之。

$(5)_1$ 当 $12<dk^2<\dfrac{49}{4}$ 成立时，这时有

$$0<-\frac{1}{4}\sqrt{dk^2+8}+\frac{5}{4}<\frac{1}{4}\sqrt{dk^2-8}\leqslant-\frac{1}{4}\sqrt{dk^2-8}+\frac{5}{4}$$

$$<\frac{1}{4}\sqrt{dk^2+8}<-\frac{1}{4}\sqrt{dk^2+8}+\frac{9}{4}.$$

因此又可区分为三种不同的情形。

$(5)_{11}$ 如有

$$-\frac{1}{4}\sqrt{dk^2+8}+\frac{5}{4}<h+N+\frac{5}{4}k\leqslant\frac{1}{4}\sqrt{dk^2-8},$$

则

$$|F(h+N,\ k-1)|<1;$$

$(5)_{12}$ 如有

$$\frac{1}{4}\sqrt{dk^2-8}<h+N+\frac{5}{4}k<\frac{1}{4}\sqrt{dk^2+8},$$

则有

$$|F(h+N,\ k)|<1;$$

$(5)_{13}$ 如有

$$\frac{1}{4}\sqrt{dk^2+8}\leqslant h+N+\frac{5}{4}k\leqslant -\frac{1}{4}\sqrt{dk^2+8}+\frac{9}{4},$$

则有

$$|F(h+N-1,\ k-1)|<1。$$

$(5)_2$ 当 $\frac{49}{4}<dk^2$ 时 $\left(\text{注意不可能有}\frac{49}{4}=dk^2\right)$，有

$$0<-\frac{1}{4}\sqrt{dk^2+8}+\frac{5}{4}<\frac{1}{4}\sqrt{dk^2-8}\leqslant -\frac{1}{4}\sqrt{dk^2-8}+\frac{5}{4}$$
$$<-\frac{1}{4}\sqrt{dk^2+8}+\frac{9}{4}<\frac{1}{4}\sqrt{dk^2+8}。$$

因此又可区分为二种不同的情形。

$(5)_{21}$ 如有

$$-\frac{1}{4}\sqrt{dk^2+8}+\frac{5}{4}<h+N+\frac{5}{4}k\leqslant\frac{1}{4}\sqrt{dk^2-8},$$

则有

$$|F(h+N,\ k-1)|<1;$$

$(5)_{22}$ 如有

$$\frac{1}{4}\sqrt{dk^2-8}<h+N+\frac{5}{4}k<\frac{1}{4}\sqrt{dk^2+8},$$

则有

$$|F(h+N,\ k)|<1。$$

综上所述，$Q(\sqrt{57})$是 Euclid 域。

(6) $d=73,\ F=4x^2+3xy-4y^2$ 时（注意 $f_{73}(34,\ 9)=4$），区分为几种情况讨论之。

$(6)_1$ 当 $dk^2<16$ 时，此时取 $N\in Z$，使

$$-\frac{1}{8}\sqrt{dk^2+16}<h+N+\frac{3}{8}k\leqslant -\frac{1}{8}\sqrt{dk^2+16}+1。$$

则有

$$|F(h+N,\ k)|<1;$$

$(6)_2$ 当 $dk^2>16$ 时（注意不可能有 $dk^2=16$），取 $N\in Z$，使

$$-\frac{1}{8}\sqrt{dk^2+16}+\frac{3}{8}<h+N+\frac{3}{8}k$$

$$\leqslant -\frac{1}{8}\sqrt{dk^2+16}+\frac{11}{8}.$$

这时有

$$-\frac{1}{8}\sqrt{dk^2+16}+\frac{3}{8}<\frac{1}{8}\sqrt{dk^2-16}$$

$$\leqslant -\frac{1}{8}\sqrt{dk^2-16}+\frac{3}{8}<-\frac{1}{8}\sqrt{dk^2+16}+\frac{11}{8}$$

$$<\frac{1}{8}\sqrt{dk^2+16}.$$

因此又可分为二种不同的情况。

$(6)_{2.1}$ 如有

$$\frac{1}{8}\sqrt{dk^2-16}<h+N+\frac{3}{8}k<\frac{1}{8}\sqrt{dk^2+16},$$

则有

$$|F(h+N,\ k)|<1;$$

$(6)_{2.2}$ 如有

$$-\frac{1}{8}\sqrt{dk^2+16}+\frac{3}{8}<h+N+\frac{3}{8}k\leqslant\frac{1}{8}\sqrt{dk^2-16},$$

则有

$$|F(h+N,\ k-1)|<1.$$

综上所述 $Q(\sqrt{73})$ 为 Euclid 域。

(7) 类似的也可以证明 $Q(\sqrt{76})$ 也是 Euclid 域，由于证明太繁琐，我们略去了。

总之，我们已证明了定理 3.2 的前一半。

3.2 Davenport 定理的证明(二)

在本小节中，我们来证明除了定理 3.2 中所列举的 16 个实二次域外，其他的实二次域均不是 Euclid 域。这是 Davenport 首先证明的。

如 §3.1 中所述，对一个给定的正的基本判别式 $d>0$，实二次域 $K=Q(\sqrt{d})$ 是否是 Euclid 域，取决于对于有理整系数二元二次型 $f_d(x,\ y)$，是否对任给的有理数对 h、k，均存在有理整

数 x、y，使

$$|f_d(x+h,\ y+k)|<1.$$

我们现在来证明，存在一对有理数 h，k 使

$$|f_d(x+h,\ y+k)|>\frac{\sqrt{d}}{31} \tag{4.122}$$

对所有的有理整数 x，y均成立。这样当$d>31^2=961$时，$Q(\sqrt{d})$就不是 Euclid 域，对 $d<961$ 的实二次域$Q(\sqrt{d})$，可以经过具体的计算证明除去定理 3.2 中列举的 16 个以外，不再存在 Euclid 域。注意我们可设 $d>5$。

首先可知，对 $(x,\ y)\in\mathbb{Z}-\{(0,\ 0)\}$，均有$|f_d(x,\ y)|\geqslant 1$，令

$$\alpha=\alpha_d=\begin{cases}\dfrac{\sqrt{d}}{2}, & \text{如 } 4|d;\\[2ex] \dfrac{1+\sqrt{d}}{2}, & \text{如 } d\equiv 1(\mathrm{mod}4).\end{cases}$$

则有

$$f_d(x,\ y)=(x+\alpha y)(x+\alpha' y), \tag{4.123}$$

其中 α' 是 α 的共轭元。可选 $n\in\mathbb{Z}$，使

$$\frac{1-\sqrt{5}}{2}<\alpha'+n\leqslant\frac{3-\sqrt{5}}{2}.$$

令

$$\theta=\alpha+n,\ \theta'=\alpha'+n.$$

则可验证下列三对数：

$$\theta,\ \theta';\ 2-\theta',\ 2-\theta;\ 1-\frac{1}{\theta'},\quad 1-\frac{1}{\theta}$$

中至少有一对满足 H-约化条件：

$$\theta>2,\ \frac{1-\sqrt{5}}{2}<\theta'<\frac{3-\sqrt{5}}{2},$$

即 θ, $2-\theta'$, $1-\dfrac{1}{\theta'}$ 中至少有一个是 H-约化的。这样可展开 θ 为奇异连分数。上述讨论说明了下列断言是成立的：

f_d 相似于 $F_0=F_0(x,\ y)=a_0(x+\theta_0 y)(x+\theta_0' y)$，这里我们必需把相似的定义予以推广，即用于相似的方阵可以是其行列式为

± 1的二阶有理整系数方阵；θ_0 是 H-约化的，实二次无理数 θ_0，$\theta_0' \in Q(\sqrt{d})$。同时存在一串有理整数

$$t_n \qquad (n \in \mathbb{Z}) \tag{4.124}$$

和一串符号 $\mu_n(=\pm 1)\ (n\in\mathbb{Z})$ 使

$$\theta_n = t_n + \frac{\mu_{n+1}}{\theta_{n+1}}, \quad \theta_n' = t_n + \frac{\mu_{n+1}}{\theta_{n+1}'} \quad (n \in \mathbb{Z}) \tag{4.125}$$

这里 θ_n' 是 θ_n 的共轭元，均 $\in Q(\sqrt{d})$，且 θ_n 是 H-约化的；μ_{n+1} 与 θ_{n+1}' 的符号相反，并且

$$F_n(x, y) = a_n(x+\theta_n y)(x+\theta_n' y)\ (n \in \mathbb{Z}) \tag{4.126}$$

相似(相似方阵的行列式$=\pm 1$)于 $F_0(x, y)$，具体的有

$$F_n(x, y) = F_{n+1}(y, \mu_{n+1}(x+t_n y)),\ n \in \mathbb{Z} \tag{4.127}$$

最后还有

(1) t_n 是离 θ_n 最近的有理整数；

(2) $t_n \geqslant 2\ (n\in\mathbb{Z})$；并且当 $\mu_{n+1}=-1$ 时，有 $t_n \geqslant 3$；

(3) 令 $\phi_n = -\dfrac{\mu_n}{\theta_n'}$，则有

$$\phi_n > 0,\ \phi_n = t_{n-1} + \frac{\mu_{n-1}}{\phi_{n-1}}\ (n \in \mathbb{Z})； \tag{4.128}$$

(4) $d = a_n^2(\theta_n - \theta_n')^2$。

以上成立的原因除上述的讨论外，还有第一章关于奇异连分数的理论。

对 $n\in\mathbb{Z}$，令

$$w_n = \begin{cases} 0, & \text{如 } t_n \text{ 偶且 } \mu_{n+1}=1; \\ 1, & \text{如 } t_n \text{ 偶且 } \mu_{n+1}=-1; \\ \dfrac{1}{2}, & \text{如 } t_n \text{ 奇}, \end{cases} \tag{4.129}$$

$$\delta_n = w_n + \sum_{i=1}^{\infty} \frac{\mu_{n+1}\mu_{n+2}\cdots\mu_{n+i}}{\theta_{n+1}\theta_{n+2}\cdots\theta_{n+i}} w_{n+i} \quad (n \in \mathbb{Z}) \tag{4.130}$$

$$\delta_n' = \frac{w_{n-1}}{\phi_n} + \sum_{i=1}^{\infty} (-1)^i \frac{w_{n-i-1}}{\phi_n\phi_{n-1}\cdots\phi_{n-i}} \quad (n \in \mathbb{Z}). \tag{4.131}$$

易见定 δ_n 与 δ_n' 的级数均是绝对收敛的，且有

$$|\delta_n|<2, \quad |\delta'_n|<\frac{3+\sqrt{5}}{2} \quad (n\in\mathbb{Z}), \tag{4.132}$$

$$\delta_n = w_n + \mu_{n+1}\frac{\delta_{n+1}}{\theta_{n+1}},$$

$$\delta'_n = w_n + \mu_{n+1}\frac{\delta'_{n+1}}{\theta'_{n+1}} \quad (n\in\mathbb{Z}). \tag{4.133}$$

由于 θ_n 是周期的，令基本周期长度为 k。则由第一章已知 $\theta_{n+1}\cdots\theta_{n+k}=\varepsilon$ 是 $Q(\sqrt{d})$ 的基本单位，$n\in\mathbb{Z}$。于是 θ'_n, ϕ_n, w_n, δ_n, δ'_n 均是周期，基本周期长度也是 k。所以

$$\delta_n = \left(w_n + \sum_{i=1}^{k-1}\frac{\mu_{n+1}\cdots\mu_{n+i}}{\theta_{n+1}\cdots\theta_{n+i}}w_{n+i}\right)\frac{1}{1-\frac{\eta}{\varepsilon}},$$

$$\eta = \mu_{n+1}\mu_{n+2}\cdots\mu_{n+k}, \ n\in\mathbb{Z}, \tag{4.134}$$

$$\delta'_n = \left(\frac{w_{n-1}}{\phi_n} + \sum_{i=1}^{k-1}(-1)^i\frac{w_{n-i-1}}{\phi_n\cdots\phi_{n-i}}\right)\frac{1}{1-\eta\varepsilon'}, \ n\in\mathbb{Z}, \tag{4.135}$$

这里 ε' 是 ε 的共轭元。

把(4.135)中的 n 换为 $n+k$，两边同乘以 $\phi_{n+1}\cdots\phi_{n+k}$，即有

$$\delta'_n\phi_{n+1}\cdots\phi_{n+k} = \left(\sum_{i=0}^{k-1}(-1)^i\phi_{n+1}\cdots\phi_{n+k-i-1}w_{n+k-i-1}\right)\frac{1}{1-\eta\varepsilon'},$$

在上式两边均取共轭，并令 δ'_n 的共轭元为 δ，则有

$$(-1)^k\frac{\eta\delta}{\varepsilon} = (-1)^{k-1}\left(w_n + \sum_{i=1}^{k-1}\frac{\mu_{n+1}\cdots\mu_{n+i}}{\theta_{n+1}\cdots\theta_{n+i}}w_{n+i}\right)\frac{1}{1-\eta\varepsilon},$$

即有

$$-\frac{\eta}{\varepsilon}\delta = \delta_n\frac{1-\frac{\eta}{\varepsilon}}{1-\eta\varepsilon}, \ \text{因此}\ \delta=\delta_n.$$

这证明了 δ'_n 即为 δ_n 的共轭元，$n\in\mathbb{Z}$。

引理 3.1 $0\leqslant\delta_n\leqslant1$, $n\in\mathbb{Z}$. (4.136)

证明 首先证明

$$\left|\frac{\delta_n}{\theta_n}\right|<\frac{1}{2}, \quad n\in\mathbb{Z}. \tag{4.137}$$

由(4.132)已知 $|\delta_n|<2$，因此由(4.133)及 θ_n 是 H-约化的，得

到：

$$\left|\frac{\delta_n}{\theta_n}\right| \leqslant \begin{cases} \left|\dfrac{\delta_n}{\theta_n\theta_{n+1}}\right| < \dfrac{1}{2}, \text{ 如 } w_n = 0; \\ \left|\dfrac{\delta_n}{\theta_n}\right| < \dfrac{2}{3.5}, \text{ 如 } w_n = 1; \\ \dfrac{\dfrac{1}{2} + \left|\dfrac{\delta_{n+1}}{\theta_{n+1}}\right|}{\theta_n} < \dfrac{\dfrac{1}{2}+1}{2.5} = \dfrac{3}{5}, \text{ 如 } w_n = \dfrac{1}{2}, \end{cases}$$

其中还用到 t_n 的性质，所以我们有

$$\left|\frac{\delta_n}{\theta_n}\right| < \frac{3}{5},\ n \in \mathbb{Z}. \tag{4.138}$$

用(4.138)、(4.133)、θ_n 是 H-约化的，以及 t_n 的性质，即得

$$\left|\frac{\delta_n}{\theta_n}\right| \leqslant \begin{cases} \left|\dfrac{\delta_{n+1}}{\theta_n\theta_{n+1}}\right| < \dfrac{3}{10}, \text{ 如 } w_n = 0; \\ \dfrac{1 + \left|\dfrac{\delta_{n+1}}{\theta_{n+1}}\right|}{\theta_n} < \dfrac{1+\dfrac{3}{5}}{3.5} < \dfrac{1}{2}, \text{ 如 } w_n = 1; \\ \dfrac{\dfrac{1}{2} + \left|\dfrac{\delta_{n+1}}{\theta_{n+1}}\right|}{\theta_n} < \dfrac{\dfrac{1}{2}+\dfrac{3}{5}}{2.5}, \text{ 如 } w_n = \dfrac{1}{2}, \end{cases}$$

这就证明(4.137)。第二步来证明

$$\delta_n \geqslant 0, \quad n \in \mathbb{Z} \tag{4.139}$$

用反证法，如果存在 $n_0 \in \mathbb{Z}$，使 $\delta_{n_0} < 0$，则由(4.137)及(4.133)即知，必有 $w_{n_0} = 0$，从而有

$$\delta_{n_0} = \frac{\delta_{n_0+1}}{\theta_{n_0+1}},$$

故由 $\delta_{n_0} < 0$，即有 $\delta_{n_0+1} < 0$，依次推导，可知，对任一个 $i \geqslant 1$ 均有

$$\delta_{n_0} = \frac{\delta_{n_0+i}}{\theta_{n_0+1}\theta_{n_0+2}\cdots\theta_{n_0+i}},\quad i \geqslant 1, \tag{4.140}$$

这样由 $|\delta_n| < 2$，$\theta_n > 2\,(n \in \mathbb{Z})$，因此在(4.140)中令 $i \to \infty$，即得 $\delta_{n_0} = 0$，这与 $\delta_{n_0} < 0$ 矛盾。这就证明了(4.139)。

由(4.129)、(4.133)、(4.137)和(4.139)即得 $\delta_n \leqslant 1$，$n \in \mathbb{Z}$。所以(4.136)完全得证。引理证毕。

推论 (1) 如存在 $n_0\in\mathbb{Z}$ 使 $\delta_{n_0}=0$, 则必有 $\delta_n=0$, $\forall n\in\mathbb{Z}$。

(2) $\delta_n<1$, $\forall n\in\mathbb{Z}$。

证明 如 $\delta_{n_0}=0$, 由上述引理证明中的第二步可得$\delta_n=0$, $\forall n\geqslant n_0$; 又如$\delta_{n_0}=1$, 同样可得$\delta_n=0$, $\forall n\geqslant n_0+1$。再由δ_n的周期性立即得到所需的结论。

引理 3.2 对任一个满足$0\leqslant\lambda\leqslant\frac{1}{2}$的正常数$\lambda$, 均有

$$\delta_n<\lambda\theta_n+1-3.5\lambda,\ n\in\mathbb{Z} \tag{4.141}$$

证明 $\lambda=0$ 时, 即为$\delta_n<1$, 这已由上述推论知道是成立的。因此由凸性可知, 只需证明 $\lambda=\frac{1}{2}$ 时的(4.141), 即应证明

$$\delta_n<\frac{1}{2}\theta_n-\frac{3}{4},\ n\in\mathbb{Z} \tag{4.142}$$

今由(4.125)、(4.133)、(4.129)、(4.136) 以及 θ_n 为 H-约化的, 即有

$$\delta_n-\frac{1}{2}\theta_n+\frac{3}{4}=w_n-\frac{1}{2}t_n+\frac{3}{4}+\frac{\mu_{n+1}}{\theta_{n+1}}\left(\delta_{n+1}-\frac{1}{2}\right)$$

$$<\begin{cases} 0-\frac{2}{2}+\frac{3}{4}+\frac{1}{2}\left(1-\frac{1}{2}\right)=0, & \text{如 } t_n \text{ 偶}, \mu_{n+1}=1; \\ 1-\frac{4}{2}+\frac{3}{4}+\frac{1}{2}\cdot\frac{1}{2}=0, & \text{如 } t_n \text{ 偶}, \mu_{n+1}=-1; \\ \frac{1}{2}-\frac{3}{2}+\frac{3}{4}+\frac{1}{2}\left(1-\frac{1}{2}\right)=0, & \text{如 } t_n \text{ 奇}, \mu_{n+1}=1; \\ \frac{1}{2}-\frac{3}{2}+\frac{3}{4}+\frac{1}{2}\cdot\frac{1}{2}=0, & \text{如 } t_n \text{ 奇}, \mu_{n+1}=-1, \end{cases}$$

这就证明了(4.142), 也就证明了引理, 即(4.141)。

引理 3.3 $0.25\theta_n'\leqslant\delta_n'\leqslant0.25,\ n\in\mathbb{Z}$ (4.143)

证明 由定义及有关性质有

$$\theta_n'=-\mu_n|\theta_n'|,\ \delta_n'=(w_{n-1}-\delta_{n-1}')|\theta_n'|,$$
$$1=(t_{n-1}-\theta_{n-1}')|\theta_n'|,\ n\in\mathbb{Z},$$

所以有

$$\delta_n'-0.25\theta_n'=(0.25-\delta_{n-1}')|\theta_n'|+(w_{n-1}-0.25+0.25\mu_n)|\theta_n'|, \tag{4.144}$$

$$0.25-\delta'_n=(\delta'_{n-1}-0.25\theta'_{n-1})|\theta'_n| + (0.25t_{n-1}-w_{n-1})|\theta'_n|. \qquad (4.145)$$

容易看到，对任一个 $n\in\mathbb{Z}$，均有

$$w_{n-1}-0.25+0.25\mu_n=\begin{cases}0, & \text{如 } t_{n-1} \text{ 偶}, \mu_n=1 \text{ 或 } t_{n-1} \text{ 奇}, \mu_n=-1;\\ 0.5, & \text{如 } t_{n-1} \text{ 偶 } \mu_n=-1 \text{ 或 } t_{n-1} \text{ 奇}, \mu_n=1\end{cases}$$

与

$$0.25t_{n-1}-w_{n-1}=\begin{cases}0.25t_{n-1}\geqslant 0.5, & \text{如 } t_{n-1} \text{ 偶}, \mu_n=1;\\ 0.25t_{n-1}-1\geqslant 0, & \text{如 } t_{n-1} \text{ 偶}, \mu_n=-1;\\ 0.25t_n-0.5\geqslant 0.25, & \text{如 } t_{n-1} \text{ 奇},\end{cases}$$

由此及(4.144)、(4.145)即得

$$\delta'_n-0.25\theta'_n\geqslant(\delta'_{n-2}-0.25\theta'_{n-2})|\theta'_n||\theta'_{n-1}|, \quad n\in\mathbb{Z}, \qquad (4.146)$$

$$0.25-\delta'_n\geqslant(0.25-\delta'_{n-2})|\theta'_n||\theta'_{n-1}|, \quad n\in\mathbb{Z}. \qquad (4.147)$$

反复运用(4.146)与(4.147)，并注意到 δ'_n 的有界性，以及

$$|\theta'_n|<\frac{\sqrt{5}-1}{2}<1,$$

知(4.143)也即引理成立。

命

$$\beta_n=\frac{1}{2}+\frac{1}{2}\theta_n-\delta_n,$$

$$\beta'_n=\frac{1}{2}+\frac{1}{2}\theta'_n-\delta'_n, \quad n\in\boldsymbol{Z} \qquad (4.148)$$

由于 θ'_n、δ'_n 分别是 θ_n、δ_n 的共轭元，故 β'_n 是 β_n 的共轭元，并且易得

$$\beta_n=v_n+\mu_{n+1}\frac{\beta_{n+1}}{\theta_{n+1}}, \quad \beta'_n=v_n+\mu_{n+1}\frac{\beta'_{n+1}}{\theta'_{n+1}}, \quad n\in\boldsymbol{Z} \qquad (4.149)$$

其中 v_n 为有理整数，且

$$v_n=\begin{cases}\dfrac{t_n}{2}, & \text{如 } t_n \text{ 偶};\\ \dfrac{t_n-\mu_{n+1}}{2}, & \text{如 } t_n \text{ 奇},\end{cases} \qquad (4.150)$$

故 v_n 为正整数，且 $\mu_{n+1}=-1$ 时，$v_n\geqslant 2$。

引理 3.4　对任一个 $n\in Z$, 均有

$$\beta_n>\frac{5}{4},\qquad \frac{\theta_n}{2}-\frac{1}{2}<\beta_n\leqslant\frac{\theta_n}{2}+\frac{1}{2},$$

$$\frac{5}{14}<\frac{\beta_n}{\theta_n}<\frac{3}{4}. \tag{4.151}$$

证明　第一个不等式, 可由 $\delta_n<\frac{1}{2}\theta_n-\frac{3}{4}$ 得出; 第二个不等式, 可由 $0\leqslant\delta_n<1$ 得出; 第三个不等式, 可由 $\delta_n<\frac{1}{7}\theta_n+\frac{1}{2}$ (在引理3.2中取 $\lambda=\frac{1}{7}$) 得出其左边, 其右边可由 $\beta_n>\frac{\theta_n-1}{2}$ 得出.

引理 3.5　我们有

$$\eta_1\theta_n'-\eta_2\leqslant\delta_n'\leqslant\lambda_1\theta_n'+\lambda_2,\ n\in Z \tag{4.152}$$

其中 λ_1, λ_2, η_1, η_2 为满足下列诸条件的实常数:

$$\frac{71+2\sqrt{6}}{346}\leqslant\lambda_2\leqslant\frac{3+\sqrt{6}}{2},$$

$$\frac{\sqrt{6}}{6}-\frac{3+2\sqrt{6}}{3}\lambda_2\leqslant\lambda_1\leqslant\frac{3-\sqrt{6}}{6}+\frac{2\sqrt{6}}{3}\lambda_2,$$

如
$$\frac{1}{2}\leqslant\lambda_2\leqslant\frac{3+\sqrt{6}}{2};$$

$$\frac{3+\sqrt{6}}{6}-\frac{6+2\sqrt{6}}{3}\lambda_2\leqslant\lambda_1\leqslant-\frac{\sqrt{6}}{6}+\frac{3+2\sqrt{6}}{6}\lambda_2,$$

如
$$\frac{1}{4}\leqslant\lambda_2\leqslant\frac{1}{2};$$

$$\frac{9+\sqrt{6}}{10}-\frac{18+2\sqrt{6}}{5}\lambda_2\leqslant\lambda_1$$

$$\leqslant-\frac{4+\sqrt{6}}{10}+\frac{13+2\sqrt{6}}{5}\lambda_2,$$

如
$$\frac{71+2\sqrt{6}}{346}\leqslant\lambda_2\leqslant\frac{1}{4}.$$

$$-\frac{3+2\sqrt{6}}{6}\leqslant\eta_1\leqslant\frac{3+\sqrt{6}}{2},$$

$$\eta_2=\begin{cases}\dfrac{2(\sqrt{6}-1)}{5}\left(\dfrac{1}{4}-\eta_1\right), & \text{如 } -\dfrac{3+2\sqrt{6}}{6}\leqslant\eta_1\leqslant\dfrac{1}{4};\\[2ex] \dfrac{2(3-\sqrt{6})}{3}\left(\eta_1-\dfrac{1}{4}\right), & \text{如 } \dfrac{1}{4}\leqslant\eta_1\leqslant\dfrac{3+\sqrt{6}}{2}.\end{cases}$$

证明　我们考虑下述的命题 $P(\rho)$.

命题 $P(\rho)$　设实数 ρ 满足 $\dfrac{1}{2}<\rho<1$, 令

$$\delta=\frac{9\rho-1}{8\rho-1},$$

则有

$$\eta_1\theta_n'-\eta_2\leqslant\delta_n'\leqslant\lambda_1\theta_n'+\lambda_2,\ n\in\mathbb{Z}$$

其中 λ_1, λ_2, η_1, η_2 为满足下述诸条件的实常数，它们仅依赖于 ρ:

$$\frac{28\rho-3}{2(64\rho-7)}\leqslant\lambda_2\leqslant3\rho,$$

$$\rho-\frac{1}{2}-(4\rho-1)\lambda_2\leqslant\lambda_1\leqslant1-\rho+(4\rho-2)\lambda_2,$$

如
$$\frac{1}{2}\leqslant\lambda_2\leqslant3\rho;$$

$$\rho-4\rho\lambda_2\leqslant\lambda_1\leqslant\frac{1}{2}-\rho+(4\rho-1)\lambda_2,$$

如
$$\frac{1}{4}\leqslant\lambda_2\leqslant\frac{1}{2};$$

$$\delta-4\delta\lambda_2\leqslant\lambda_1\leqslant\frac{1}{2}-\delta+(4\delta-1)\lambda_2,$$

如
$$\frac{28\rho-3}{2(64\rho-7)}\leqslant\lambda_2\leqslant\frac{1}{4}.$$

$$-2\rho+\frac{1}{2}\leqslant\eta_1\leqslant3\rho,$$

$$\eta_2=\begin{cases}\dfrac{4\rho}{8\rho-1}\left(\dfrac{1}{4}-\eta_1\right), & \text{如 } -2\rho+\dfrac{1}{2}\leqslant\eta_1\leqslant\dfrac{1}{4};\\[2ex] \dfrac{4\rho}{12\rho-1}\left(\eta_1-\dfrac{1}{4}\right), & \text{如 } \dfrac{1}{4}\leqslant\eta_1\leqslant3\rho.\end{cases}$$

注意:

$\left(\frac{9\rho-1}{64\rho-7},\ \frac{28\rho-3}{2(64\rho-7)}\right)$ 为 $\lambda_1-\lambda_2$ 平面上的两条直线 $\lambda_1=\rho-4\rho\lambda_2$ 与 $\lambda_1=\frac{1}{2}-\rho+(4\rho-1)\lambda_2$ 的交点。

第一步，我们来证明命题 $P\left(\frac{5+\sqrt{5}}{8}\right)$是成立的。

由引理 3.3 已知 $\theta'_n\leqslant 4\delta'_n$，故仿引理 3.3 的证明有

$$\delta'_n-\lambda_1\theta'_n-\lambda_2=|\theta'_n|(w_{n-1}-\delta'_{n-1}+\mu_n\lambda_1-\lambda_2(t_{n-1}-\theta'_{n-1}))$$
$$\leqslant|\theta'_n|(w_{n-1}+\mu_n\lambda_1-t_{n-1}\lambda_2+(\lambda_2-0.25)\theta'_{n-1}),$$

因此当 $\lambda_2\geqslant\frac{1}{4}$ 时，有(注意 $\phi_n=|\theta'_n|^{-1}>0$)

$$\phi_n(\delta'_n-\lambda_1\theta'_n-\lambda_2)\leqslant w_{n-1}+\mu_n\lambda_1-t_{n-1}\lambda_2+(\lambda_2-0.25)\frac{3-\sqrt{5}}{2}$$

$$\leqslant\begin{cases}\lambda_1-2\lambda_2+(\lambda_2-0.25)\frac{3-\sqrt{5}}{2}, & \text{如 } t_{n-1}\text{ 偶}, \mu_n=1;\\ 1-\lambda_1-4\lambda_2+(\lambda_2-0.25)\frac{3-\sqrt{5}}{2}, & \text{如 } t_{n-1}\text{ 偶}, \mu_n=-1;\\ \frac{1}{2}+\lambda_1-3\lambda_2+(\lambda_2-0.25)\frac{3-\sqrt{5}}{2}, & \text{如 } t_{n-1}\text{ 奇}, \mu_n=1;\\ \frac{1}{2}-\lambda_1-3\lambda_2+(\lambda_2-0.25)\frac{3-\sqrt{5}}{2}, & \text{如 } t_{n-1}\text{ 奇}, \mu_n=-1,\end{cases}$$

所以当 $\lambda_2\geqslant\frac{1}{2}$ 时，只需满足

$$\lambda_1-2\lambda_2+(\lambda_2-0.25)\frac{3-\sqrt{5}}{2}\leqslant 0$$
$$\leqslant-\frac{1}{2}+\lambda_1+3\lambda_2-(\lambda_2-0.25)\frac{3-\sqrt{5}}{2}, \tag{4.153}$$

而当 $\frac{1}{4}\leqslant\lambda_2\leqslant\frac{1}{2}$ 时，只需满足

$$\frac{1}{2}+\lambda_1-3\lambda_2+(\lambda_2-0.25)\frac{3-\sqrt{5}}{2}\leqslant 0$$
$$\leqslant-1+\lambda_1+4\lambda_2-(\lambda_2-0.25)\frac{3-\sqrt{5}}{2}, \tag{4.154}$$

即有

$$\delta'_n \leqslant \lambda_1 \theta'_n + \lambda_2, \tag{4.155}$$

又易知(4.153)与(4.154) 即为命题 $P\left(\frac{5+\sqrt{5}}{8}\right)$中 $\lambda_2 \geqslant \frac{1}{4}$ 时所给出的条件。故我们已证明，当 $\lambda_2 \geqslant \frac{1}{4}$ 时，如λ_1满足$P\left(\frac{5+\sqrt{5}}{8}\right)$所给条件时，(4.155)成立。特别取

$$\frac{1}{4} \leqslant \lambda_2 \leqslant \frac{1}{2}, \qquad \lambda_1 = \frac{5+\sqrt{5}}{8} - \frac{5+\sqrt{5}}{2} \lambda_2,$$

即有：

[事实 I] 如有

$$\lambda = \frac{1}{4} + \frac{5-\sqrt{5}}{10} \delta, \quad 0 \leqslant \delta \leqslant \frac{5+\sqrt{5}}{8},$$

则有

$$\delta'_n \leqslant -\delta \theta'_n + \lambda, \ n \in \mathbb{Z}.$$

命题 $P\left(\frac{5+\sqrt{5}}{8}\right)$中，$\eta_1$，$\eta_2$ 所满足的条件为

$$\eta_2 = \begin{cases} \frac{15-\sqrt{5}}{22}\left(\frac{1}{4} - \eta_1\right), & \text{如 } -\frac{3+\sqrt{5}}{4} \leqslant \eta_1 \leqslant \frac{1}{4}; \\ \frac{25-\sqrt{5}}{62}\left(\eta_1 - \frac{1}{4}\right), & \text{如 } \frac{1}{4} \leqslant \eta_1 \leqslant \frac{15+3\sqrt{5}}{8}. \end{cases}$$

因此当 $-\frac{3+\sqrt{5}}{4} \leqslant \eta_1 \leqslant \frac{15+3\sqrt{5}}{8}$ 时，有

$$0 \leqslant \eta_2 \leqslant \frac{5+\sqrt{5}}{8}.$$

易见当 $-\frac{3+\sqrt{5}}{4} \leqslant \eta_1 \leqslant \frac{1}{4}$ 时，有

$$\eta_1 = \frac{1}{4} - \frac{15+\sqrt{5}}{10} \eta_2,$$

故由事实 I 得出（取 $\delta = \eta_2$）：

$$\begin{aligned} (\delta'_n - \eta_1 \theta'_n + \eta_2)\phi_n &= w_{n-1} - \delta'_{n-1} + \mu_n \eta_1 + \eta_2 (t_{n-1} - \theta'_{n-1}) \\ &\geqslant w_{n-1} - \lambda + \mu_n \eta_1 + \eta_2 t_{n-1} \end{aligned}$$

$$\geqslant\begin{cases}-\lambda+\eta_1+2\eta_2=0, & \text{如 } t_{n-1} \text{ 偶}, \mu_n=1;\\ 1-\lambda-\eta_1+4\eta_2\geqslant\frac{1}{2}, & \text{如 } t_{n-1} \text{ 偶}, \mu_n=-1;\\ \frac{1}{2}-\lambda+\eta_1+3\eta_2\geqslant\frac{1}{2}, & \text{如 } t_{n-1} \text{ 奇}, \mu_n=1;\\ \frac{1}{2}-\lambda-\eta_1+3\eta_2\geqslant 0, & \text{如 } t_{n-1} \text{ 奇}, \mu_n=-1,\end{cases}$$

这证明了

$$\delta'_n\geqslant\eta_1\theta'_n-\eta_2,\ n\in Z. \tag{4.156}$$

也即证明了命题 $P\left(\frac{5+\sqrt{5}}{8}\right)$，当 $-\frac{3+\sqrt{5}}{8}\leqslant\eta_1\leqslant\frac{1}{4}$ 时的相应结论。

而当 $\frac{1}{4}\leqslant\eta_1\leqslant\frac{15+3\sqrt{5}}{8}$ 时，$\eta_1=\frac{1}{4}+\frac{25+\sqrt{5}}{10}\eta_2$，因此与上同法可以证明命题 $P\left(\frac{5+\sqrt{5}}{8}\right)$中，当 $\frac{1}{4}\leqslant\eta_1\leqslant\frac{15+3\sqrt{5}}{8}$ 时的相应结论。总之，已证明了命题 $P\left(\frac{5+\sqrt{5}}{8}\right)$ 中的结论(4.156)。特别的有：

[事实 I] $\delta'_n\geqslant\lambda_2\theta'_n-\lambda$, $n\in Z$，如

$$\lambda=\frac{15-\sqrt{5}}{22}\left(\frac{1}{4}-\lambda_2\right),\quad 0\leqslant\lambda_2\leqslant\frac{1}{4}.$$

由事实 I 可知，当 $0\leqslant\lambda_2\leqslant\frac{1}{4}$ 时，有

$$\begin{aligned}\phi_n(\delta'_n-\lambda_1\theta_n-\lambda_2)&=w_{n-1}-\delta'_{n-1}+\mu_n\lambda_1-\lambda_2(t_{n-1}-\theta'_{n-1})\\ &\leqslant w_{n-1}+\lambda+\mu_n\lambda_1-\lambda_2t_{n-1}\\ &\leqslant\begin{cases}\lambda+\lambda_1-2\lambda_2, & \text{当 } t_{n-1} \text{ 偶}, \mu_n=1;\\ 1+\lambda-\lambda_1-4\lambda_2, & \text{当 } t_{n-1} \text{ 偶}, \mu_n=-1;\\ \frac{1}{2}+\lambda+\lambda_1-3\lambda_2, & \text{当 } t_{n-1} \text{ 奇}, \mu_n=1;\\ \frac{1}{2}+\lambda-\lambda_1-3\lambda_2, & \text{当 } t_{n-1} \text{ 奇}, \mu_n=-1,\end{cases}\end{aligned}$$

因此为得到 $\delta'_n\leqslant\lambda_1\theta'_n+\lambda_2$，只需 λ_1 满足

$$1+\lambda-\lambda_1-4\lambda_2\leqslant 0\leqslant -\frac{1}{2}-\lambda-\lambda_1+3\lambda_2,$$

易见此即命题 $P\left(\frac{5+\sqrt{5}}{8}\right)$中，当 $\lambda_2\leqslant\frac{1}{4}$ 时，λ_1所应满足的条件，而 $\left(\frac{861+\sqrt{5}}{6152}, \frac{677-\sqrt{5}}{3076}\right)$是 $\lambda_1-\lambda_2$ 平面上两条直线$\lambda_1=\rho-4\rho\lambda_2$ 与 $\lambda_1=\frac{1}{2}-\rho+(4\rho-1)\lambda_2$ 的交点，此时 $\rho=\frac{5+\sqrt{5}}{8}$，于是可知有

$$\frac{677-\sqrt{5}}{3076}=\frac{28\rho-3}{2(64\rho-7)}\leqslant\lambda_2\leqslant\frac{1}{4}.$$

综上所述，命题 $P\left(\frac{5+\sqrt{5}}{8}\right)$已完全证明了。

第二步，我们再来证明，如满足$\frac{1}{2}<\rho<1$ 的实常数 ρ，使命题 $P(\rho)$ 成立，则当

$$\rho^*\stackrel{\text{def}}{=\!=}\frac{11\rho-1}{12\rho-1}\geqslant\rho$$

成立时，命题 $P(\rho^*)$也成立。

我们首先指出有：

$$\frac{9}{10}<\rho^*<\frac{10}{11},\quad \rho=\frac{1-\rho^*}{11-12\rho^*}.$$

由命题 $P(\rho)$有：对一切 $n\in Z$，均有：

$$\delta_n'\geqslant\lambda_2\theta_n'-\lambda,\quad 如\ \frac{1}{4}\leqslant\lambda_2\leqslant 3\rho,\quad \lambda=\frac{4\rho}{12\rho-1}\left(\lambda_2-\frac{1}{4}\right),$$

由此即知，当 $\frac{1}{4}\leqslant\lambda_2\leqslant 3\rho$ 时，有

$$\begin{aligned}\phi_n(\delta_n'-\lambda_1\theta_n'-\lambda_2)&=w_{n-1}-\delta_{n-1}'+\mu_n\lambda_1-\lambda_2(t_n-\theta_{n-1}')\\&\leqslant w_{n-1}+\lambda+\mu_n\lambda_1-\lambda_2t_{n-1}\\&\leqslant\begin{cases}\lambda+\lambda_1-2\lambda_2, & 如\ t_{n-1}\ 偶, \mu_n=1;\\ 1+\lambda-\lambda_1-4\lambda_2, & 如\ t_{n-1}\ 偶, \mu_n=-1;\\ \frac{1}{2}+\lambda+\lambda_1-3\lambda_2, & 如\ t_{n-1}\ 奇, \mu_n=1;\end{cases}\end{aligned}$$

$$\left\{ \frac{1}{2}+\lambda-\lambda_1-3\lambda_2,\ \text{如}\ t_{n-1}\ \text{奇},\ \mu_n=-1, \right.$$

所以，当 $\frac{1}{4}\leqslant\lambda_2\leqslant\frac{1}{2}$ 时，为得到

$$\delta'_n\leqslant\lambda_1\theta'_n+\lambda_2,$$

只需 λ_1 满足

$$1+\lambda-\lambda_1-4\lambda_2\leqslant 0\leqslant-\frac{1}{2}-\lambda-\lambda_1+3\lambda_2,$$

也即

$$\rho^*-4\rho^*\lambda_2\leqslant\lambda_1\leqslant\frac{1}{2}-\rho^*+(4\rho^*-1)\lambda_2,\quad \rho^*=\frac{11\rho-1}{12\rho-1},$$

此即命题 $P(\rho^*)$ 中，当 $\frac{1}{4}\leqslant\lambda_2\leqslant\frac{1}{2}$ 时，λ_1 所应满足的条件，因此命题 $P(\rho^*)$ 中，当 $\frac{1}{4}\leqslant\lambda_2\leqslant\frac{1}{2}$ 时的相应结论成立。同样的，当 $\frac{1}{2}\leqslant\lambda_2\leqslant 3\rho$ 时，为得到 $\delta'_n\leqslant\lambda_1\theta'_n+\lambda_2$，只需 λ_1 满足

$$\lambda+\lambda_1-2\lambda_2\leqslant 0\leqslant-\frac{1}{2}-\lambda+\lambda_1+3\lambda_2,$$

也即

$$\rho^*-\frac{1}{2}-(4\rho^*-1)\lambda_2\leqslant\lambda_1\leqslant 1-\rho^*+(4\rho^*-2)\lambda_2,$$

此即命题 $P(\rho^*)$ 中，当 $\frac{1}{2}\leqslant\lambda_2\leqslant 3\rho$ 时，λ_1 所应满足的条件， 因此命题 $P(\rho^*)$ 中，当 $\frac{1}{2}\leqslant\lambda_2\leqslant 3\rho$ 时的相应结论成立。

这样命题 $P(\rho^*)$ 中，当 $\frac{1}{4}\leqslant\lambda_2\leqslant 3\rho$ 时，相应的结论

$$\delta'_n\leqslant\lambda_1\theta'_n+\lambda_2,\ n\in\mathbb{Z}$$

已经成立。特别的有

[事实 I] $\delta'_n\leqslant-\delta\theta'_n+\lambda,\ n\in\mathbb{Z}$，如

$$0\leqslant\delta\leqslant\rho^*,\quad \lambda=\frac{1}{4}+\frac{\delta}{4\rho^*}.$$

当命题 $P(\rho^*)$ 中 η_1，η_2 的相应条件满足时，易见有 $0\leqslant\eta_2\leqslant\rho^*$，令 $\lambda=\frac{1}{4}+\frac{\eta_2}{4\rho^*}$，则由事实 I 可得

$$\phi_n(\delta'_n-\eta_1\theta'_n+\eta_2)=w_{n-1}-\delta'_{n-1}+\mu_n\eta_1+\eta_2(t_{n-1}-\theta'_{n-1})$$

$$\geqslant w_{n-1}-\lambda+\mu_n\eta_1+t_{n-1}\eta_2$$

$$\geqslant\left\{\begin{array}{l}-\lambda+\eta_1+2\eta_2,\ \text{当 } t_{n-1}\text{ 偶},\mu_n=1;\\ 1-\lambda-\eta_1+4\eta_2,\ \text{当 } t_{n-1}\text{ 偶},\mu_n=-1;\\ \frac{1}{2}-\lambda+\eta_1+3\eta_2,\ \text{当 } t_{n-1}\text{ 奇},\mu_n=1;\\ \frac{1}{2}-\lambda-\eta_1+3\eta_2,\ \text{当 } t_{n-1}\text{ 奇},\mu_n=-1\end{array}\right\}\geqslant 0,$$

因此命题 $P(\rho^*)$ 中，当 $-2\rho^*+\frac{1}{2}\leqslant\eta_1\leqslant 3\rho^*$ 时的相应结论

$$\delta'_n\geqslant\eta_1\theta'_n-\eta_2,\ n\in\mathbb{Z}$$

已经成立。

特别的，由于从 $\rho^*\geqslant\rho$ 可得

$$\frac{4\rho^*}{12\rho^*-1}\leqslant\frac{4\rho}{12\rho-1},$$

因此有

[事实 IV] $\delta'_n\geqslant\lambda_2\theta'_n-\lambda,\ n\in\mathbb{Z}$，如

$$\frac{1}{4}\leqslant\lambda_2\leqslant 3\rho^*,\quad \lambda=\frac{4\rho}{12\rho-1}\left(\lambda_2-\frac{1}{4}\right).$$

由事实 IV，仿上可知，命题 $P(\rho^*)$ 中，当 $\frac{1}{2}\leqslant\lambda_2\leqslant 3\rho^*$ 时相应结论

$$\delta'_n\leqslant\lambda_1\theta'_n+\lambda_2,\ n\in\mathbb{Z}$$

也是成立的。这样只剩下来证明，命题 $P(\rho^*)$ 中，当

$$\frac{28\rho^*-3}{2(64\rho^*-7)}\leqslant\lambda_2\leqslant\frac{1}{4}$$

时的相应结论

$$\delta'_n\leqslant\lambda_1\theta'_n+\lambda_2,\ n\in\mathbb{Z}.$$

由已经证明的，我们有：

[事实 V] $\delta'_n\geqslant\lambda_2\theta'_n-\lambda,\ n\in\mathbb{Z}$，如

$$0\leqslant\lambda_2\leqslant\frac{1}{4},\quad \lambda=\frac{4\rho^*}{8\rho^*-1}\left(\frac{1}{4}-\lambda_2\right).$$

因此，由事实 V，当 $0\leqslant\lambda_2\leqslant\frac{1}{4}$ 时，有

$$\begin{aligned}\phi_n(\delta'_n-\lambda_1\theta'_n-\lambda_2)&=w_{n-1}-\delta'_{n-1}+\mu_n\lambda_1-\lambda_2(t_{n-1}-\theta'_{n-1})\\&\leqslant w_{n-1}+\lambda+\mu_n\lambda_1-t_{n-1}\lambda_2\\&\leqslant\begin{cases}\lambda+\lambda_1-2\lambda_2, & \text{如 } t_{n-1} \text{ 偶}, \mu_n=1;\\1+\lambda-\lambda_1-4\lambda_2, & \text{如 } t_{n-1} \text{ 偶}, \mu_n=-1;\\\dfrac{1}{2}+\lambda+\lambda_1-3\lambda_2, & \text{如 } t_{n-1} \text{ 奇}, \mu_n=1;\\\dfrac{1}{2}+\lambda-\lambda_1-3\lambda_2, & \text{如 } t_{n-1} \text{ 奇}, \mu_n=-1,\end{cases}\end{aligned}$$

于是，$0\leqslant\lambda_2\leqslant\frac{1}{4}$ 时，$\delta'_n\leqslant\lambda_1\theta'_n+\lambda_2$ 成立的充分条件是

$$1+\lambda-4\lambda_2\leqslant\lambda_1\leqslant-\frac{1}{2}-\lambda+3\lambda_2,$$

也即

$$\delta^*-4\delta^*\lambda_2\leqslant\lambda_1\leqslant\frac{1}{2}-\delta^*+(4\delta^*-1)\lambda_2,$$

$$\delta^*=\frac{9\rho^*-1}{8\rho^*-1},$$

此即命题 $P(\rho^*)$ 中，

$$\frac{28\rho^*-3}{2(64\rho^*-1)}\leqslant\lambda_2\leqslant\frac{1}{4}$$

时，λ_1 所应满足的条件。这样我们证明了剩下的要求。

因此可知，当命题 $P(\rho)$ 成立时，只要

$$\rho^*\stackrel{\text{def}}{=\!=}\frac{11\rho-1}{12\rho-1}\geqslant\rho$$

成立，命题$P(\rho^*)$也成立。

第三步，我们从 $\rho_0=\frac{5+\sqrt{5}}{8}=0.9\cdots$ 出发，按第二步反复推导，可知命题 $P(\rho_n)$ 成立，其中实数 ρ_n 满足

$$\rho_{n+1}=\frac{11\rho_n-1}{12\rho_n-1}\geqslant\rho_n,\quad n\geqslant0.$$

序列 $\{\rho_n\}$ 递增有界 $\left(\leqslant\frac{10}{11}\right)$，故极限 ρ 存在，ρ 满足

$$\rho=\frac{11\rho-1}{12\rho-1},\ \text{故}\ \rho=\frac{3+\sqrt{6}}{6}.$$

所以命题

$$P(\rho)=P\left(\frac{3+\sqrt{6}}{6}\right)$$

成立，此即引理。

推论 对一切 $n\in\mathbb{Z}$，均有

$$\frac{1}{2}\theta_n'-\frac{3-\sqrt{6}}{6}\leqslant\delta_n'\leqslant\frac{1}{2}\theta_n'+\frac{\sqrt{6}+1}{10},$$

$$\frac{\sqrt{6}-1}{5}\theta_n'-\frac{7\sqrt{6}-17}{10}\leqslant\delta_n'\leqslant\frac{\sqrt{6}-1}{10}(2-\theta_n'),$$

$$-\frac{\sqrt{6}-1}{10}\leqslant\delta_n'\leqslant-\frac{3}{2}\theta_n'+\frac{\sqrt{6}-1}{2},$$

$$-\frac{1}{2}\theta_n'-\frac{3(\sqrt{6}-1)}{10}\leqslant\delta_n'\leqslant-\frac{1}{2}\theta_n'+\frac{4-\sqrt{6}}{4},$$

$$\delta_n'\geqslant\frac{6\sqrt{6}-11}{10}\theta_n'+\frac{51-21\sqrt{6}}{10},\ \delta_n'\geqslant 0.199\theta_n'-0.03.$$

引理 3.6 我们有

$$-\frac{\sqrt{6}-1}{10}\leqslant\frac{\delta_n-\delta_n'}{\theta_n-\theta_n'}\leqslant\frac{\sqrt{6}-1}{5},\ n\in\mathbb{Z}.$$

证明 在引理 3.2 中，取 $\lambda=\frac{\sqrt{6}-1}{5}$，则有

$$\delta_n\leqslant\frac{\sqrt{6}-1}{5}\theta_n-\frac{7\sqrt{6}-17}{10},$$

由此结合引理 3.5 推论中第二个不等式的左端，即得引理 3.6 中不等式的右端；又由引理3.5推论中第二个不等式的右端及$\theta_n>2$，即得引理 3.6 中不等式的左端。引理证毕。

引理 3.7 对一切 $n\in\mathbb{Z}$，均有

$$\frac{7-2\sqrt{6}}{10}\leqslant\frac{\beta_n-\beta_n'}{\theta_n-\theta_n'}\leqslant\frac{4+\sqrt{6}}{10},$$

$$\frac{6-\sqrt{6}}{10}\leqslant 1-\frac{\beta_n-\beta_n'}{\theta_n-\theta_n'}\leqslant\frac{3+2\sqrt{6}}{10},$$

$$\frac{4-\sqrt{6}}{10}\leqslant\beta_n'\leqslant\frac{6-\sqrt{6}}{6},$$

$$1-\beta_n'\geqslant\frac{7-2\theta_n'}{8+3\sqrt{6}}.$$

证明　第一个不等式由定义(4.148)及引理 3.6 可得，第二个不等式是第一个的推论，第三个不等式是定义(4.148)及引理 3.5 推论中第一个不等式的推论，最后一个不等式由引理 3.5 推论中的倒数第二个不等式得出。引理证毕。

令 h_0, k_0 为由下列方程

$$h_0+\theta_0k_0=\beta_0,\ h_0+\theta_0'k_0=\beta_0'$$

给出。易见 h_0, k_0 为一对有理数。我们来证明

$$|F_0(x+h_0,\ y+k_0)|\geqslant\frac{\sqrt{d}}{16+6\sqrt{6}},\quad x,\ y\in\mathbb{Z}. \tag{4.157}$$

用反证法。假设存在一对有理整数 x_0, y_0 使

$$|F_0(x_0+h_0,\ y_0+k_0)|<\frac{\sqrt{d}}{16+6\sqrt{6}},$$

则由(4.126)即有

$$|(x_0+\theta_0y_0+\beta_0)(x_0+\theta_0'y_0+\beta_0')|<\frac{\theta_0-\theta_0'}{16+6\sqrt{6}},$$

由此以及上述 θ_n, β_n 的构造，即知，有

$$|(x_n+\theta_ny_n+\beta_n)(x_n+\theta_n'y_n+\beta_n')|<\frac{\theta_n-\theta_n'}{16+6\sqrt{6}},\quad n\in\mathbb{Z}, \tag{4.158}$$

其中有理整数 x_n, y_n 由

$$x_{n+1}=y_n,\ y_{n+1}=\mu_{n+1}(x_n+t_ny_n+v_n) \tag{4.159}$$

确定。

由此，我们断定，存在有理整数 n、x、y，使

$$\begin{cases} |x+\theta_ny+\beta_n|<\dfrac{1}{\sqrt{16+6\sqrt{6}}}\sqrt{\theta_n(\theta_n-\theta_n')}, \\ |x+\theta_n'y+\beta_n'|<\dfrac{1}{\sqrt{16+6\sqrt{6}}}\sqrt{\theta_n(\theta_n-\theta_n')}, \end{cases} \tag{4.160}$$

$$\left| \,|(x+\theta_n y+\beta_n)(x+\theta'_n y+\beta'_n)| < \frac{\theta_n-\theta'_n}{16+6\sqrt{6}}. \right.$$

命

$$L_n = x_n+\theta_n y_n+\beta_n,\ L'_n = x_n+\theta'_n y_n+\beta'_n,\ n\in\mathbb{Z}, \tag{4.161}$$

则由(4.158)知有

$$|L_nL'_n| < \frac{\theta_n-\theta'_n}{16+6\sqrt{6}}, \qquad L_n = \frac{\mu_{n+1}}{\theta_{n+1}}L_{n+1},$$

$$L'_n = \frac{\mu_{n+1}}{\theta'_{n+1}}L'_{n+1},\ n\in\mathbb{Z}. \tag{4.162}$$

如对所有的 $n\in\mathbb{Z}$，均有 $L_n\neq 0$，则

$$\left|\frac{L_{n+1}}{L_n}\right| = \theta_{n+1} > 2,$$

所以有

$$|L_n|\to 0,\ 当\ n\to-\infty;\ |L_n|\to+\infty,\ 当\ n\to+\infty,$$

从而正好存在一个 $n\in\mathbb{Z}$，使

$$|L_{n-1}| < \sqrt{\frac{\theta_n-\theta'_n}{(16+6\sqrt{6})\theta_n}} < |L_n|, \tag{4.163}$$

这样有

$$|L_n| = \theta_n|L_{n-1}| < \sqrt{\frac{\theta_n(\theta_n-\theta'_n)}{16+6\sqrt{6}}}, \tag{4.164}$$

并由(4.162)的第一式以及(4.163)可得

$$|L'_n| < \sqrt{\frac{\theta_n(\theta_n-\theta'_n)}{16+6\sqrt{6}}}, \tag{4.165}$$

因此(4.164)、(4.165)以及(4.162)的第一式说明(4.160)已成立。

如存在一个 $n\in\mathbb{Z}$，使 $L_n=0$，则由(4.162)即知

$$L_n = 0,\ \forall n\in\mathbb{Z}.$$

再由 $|L'_{n+1}| = |\theta'_{n+1}|\,|L'_n|$，以及 $|\theta'_{n+1}| \leqslant \frac{\sqrt{5}-1}{2} < 1$ 即知，只需取 n 充分大，(4.160)也成立。

总之，我们已证明了(4.160)是成立的。

对满足 $rs<\rho_1$，$r<\rho_2$，$s<\rho_2$ 的非负实数 r，s 与正实数 ρ_1，ρ_2，显然有

$$r+s<\rho_2+\frac{\rho_1}{\rho_2}$$

(考 虑 $0<(\rho_2-r)(\rho_2-s)=\rho_2^2-\rho_2(r+s)+rs<\rho_2^2-\rho_2(r+s)+\rho_1$)。由这一简单的事实及(4.160)可得

$$\left|y+\frac{\beta_n-\beta_n'}{\theta_n-\theta_n'}\right|<\frac{1}{\sqrt{16+6\sqrt{6}}}\cdot\frac{1+\theta_n^{-1}}{\sqrt{1-\theta_n'\theta_n^{-1}}}$$

$$<\frac{1+\frac{1}{2}}{\sqrt{16+6\sqrt{6}}\sqrt{1-\frac{3-\sqrt{5}}{4}}}$$

$$<0.301。\tag{4.166}$$

由引理 3.7 可知,$y\leqslant-2$ 或 $y\geqslant1$ 时,有

$$\left|y+\frac{\beta_n-\beta_n'}{\theta_n-\theta_n'}\right|>1,$$

由此及(4.166)即知必有

$$y=0 \text{ 或 } -1。$$

如 $y=-1$,则由引理 3.7 可知:

$$\left|y+\frac{\beta_n-\beta_n'}{\theta_n-\theta_n'}\right|=1-\frac{\beta_n-\beta_n'}{\theta_n-\theta_n'}>\frac{6-\sqrt{6}}{10}>0.355,$$

由此及(4.166)即知 $y\neq-1$。故必有 $y=0$。

这样,由(4.160)、(4.166)及 $y=0$,即知有

$$\beta_n-\beta_n'<0.301(\theta_n-\theta_n'),\tag{4.167}$$

$$|x+\beta_n|<\sqrt{\frac{\theta_n(\theta_n-\theta_n')}{16+6\sqrt{6}}},\tag{4.168}$$

$$|x+\beta_n'|<\sqrt{\frac{\theta_n(\theta_n-\theta_n')}{16+6\sqrt{6}}},\tag{4.169}$$

$$|(x+\beta_n)(x+\beta_n')|<\frac{\theta_n-\theta_n'}{16+6\sqrt{6}}.\tag{4.170}$$

于是由引理 3.5 推论的最后一个不等式以及 (4.148)、(4.167)、引理 3.1 的推论(2)(即 $\delta_n<1$),可得

$$0.53>0.5+0.199\theta_n'-\delta_n'=\beta_n'-0.301\theta_n'>\beta_n-0.301\theta_n$$
$$=0.5+0.199\theta_n-\delta_n>-0.5+0.199\theta_n,$$

从而

$$0.199\theta_n<1.03,\ \theta_n<5.18, \tag{4.171}$$

这样，由此及(4.169)，即有

$$|x|<\beta_n'+\sqrt{\frac{\theta_n(\theta_n-\theta_n')}{16+6\sqrt{6}}}<\frac{6-\sqrt{6}}{6}$$
$$+\sqrt{\frac{5.18\left(5.18+\frac{\sqrt{5}-1}{2}\right)}{16+6\sqrt{6}}}<1.6,$$

其中用到

$$\beta_n'<\frac{6-\sqrt{6}}{6},\quad \theta_n'>-\frac{\sqrt{5}-1}{2},$$

这分别由引理 3.7 与 θ_n 是 H-约化的可得。因此我们有

$$x=0,\ \pm 1 \tag{4.172}$$

如 $x=1$，则由引理 3.7、(4.169)和(4.171)可得

$$1<1+\frac{4-\sqrt{6}}{10}\leqslant x+\beta_n'<\sqrt{\frac{\theta_n(\theta_n-\theta_n')}{16+6\sqrt{6}}}$$
$$<\sqrt{\frac{5.18\left(5.18+\frac{\sqrt{5}-1}{2}\right)}{16+6\sqrt{6}}}<0.99,$$

这是一个矛盾，故 $x\neq 1$。如 $x=0$，则由(4.168)及(4.171)可得

$$\beta_n<1,$$

这与 $\beta_n>\frac{5}{4}$(引理3.4的第一式)矛盾。所以 $x\neq 0$。这样由(4.172)有 $x=-1$。并由(4.170)即有

$$(\beta_n-1)(1-\beta_n')<\frac{\theta_n-\theta_n'}{16+6\sqrt{6}}, \tag{4.173}$$

注意，由引理 3.7 有 $\beta_n'<1$，以及由该引理的最后一式和 (4.173) 可得

$$\beta_n-1<\frac{\theta_n-\theta_n'}{14-4\theta_n'}. \tag{4.174}$$

但由 $0\leqslant\delta_{n+1}<1$，$|\theta_n'|<1$ 可得(并用到(4.148))

$$(14-4\theta_n')(\beta_n-1)-(\theta_n-\theta_n')$$

$$
\begin{aligned}
&= (6-2\theta_n')\theta_n - (14-4\theta_n')\delta_n - 7 + 3\theta_n' \\
&= (6-2\theta_n')t_n - (14-4\theta_n')w_n - 7 + 3\theta_n' \\
&\quad + \frac{\mu_{n+1}}{\theta_{n+1}}(6-2\theta_n' - (14-4\theta_n')\delta_{n+1})
\end{aligned}
$$

$$
\geqslant \begin{cases}
2(6-2\theta_n') - 7 + 3\theta_n' + \dfrac{1}{2}(6-2\theta_n' - (14-4\theta_n')) \\
\qquad = 1,\ \text{如 } t_n \text{ 偶}, \mu_{n+1} = 1; \\
4(6-2\theta_n') - (14-4\theta_n') - 7 + 3\theta_n' - \dfrac{1}{2}(6-2\theta_n') \\
\qquad = 0,\ \text{如 } t_n \text{ 偶}, \mu_{n+1} = -1; \\
3(6-2\theta_n') - \dfrac{1}{2}(14-4\theta_n') - 7 + 3\theta_n' + \dfrac{1}{2}(6-2\theta_n' - (14 \\
\qquad -4\theta_n')) = 0,\ \text{如 } t_n \text{ 奇},\ \mu_{n+1} = 1; \\
3(6-2\theta_n') - \dfrac{1}{2}(14-4\theta_n') - 7 + 3\theta_n' - \dfrac{1}{2}(6-2\theta_n') \\
\qquad = 1,\ \text{如 } t_n \text{ 奇}, \mu_{n+1} = -1,
\end{cases}
$$

即有 $(14-4\theta_n')(\beta_n-1)-(\theta_n-\theta_n')\geqslant 0$，这与(4.174)矛盾。这证明了 $x=0$ 也不可能。这样我们就完成了(4.157)的证明。

由 f_d 与 F_0 的相似性（相似方阵的行列式 $=\pm 1$），可知我们已证明了存在一对有理数 h、k，使

$$
|f_d(x+h,\ y+k)| \geqslant \frac{\sqrt{d}}{16+6\sqrt{6}},\ x,\ y\in\mathbb{Z}.
$$

今 $(16+6\sqrt{6})^2<943$。这就证明了：当 $d>943$ 时，实二次域 $Q(\sqrt{d})$ 决不是Euclid域。对于 $0<d\leqslant 943$ 的实二次域 $Q(\sqrt{d})$，证明除去上述定理 3.2 中所列举的 16 个域以外的域不是 Euclid 域，是一个可以在计算机上很快实现的。我们不再叙述了，可参见参考文献[15]。

本 章 评 注

1. Siegel-Tatuzawa 定理是一个很基本的工具。它的内容可参阅文献[86]。

2．定理1.3的证明基于参考文献[34]与[100]，它改进了参考文献[34]。

3．定理2.1采自参考文献[54]，我们在此给出了更为明确的证明。

4．在Davenport定理证明的第二部分的关键是(4.157)。

Davenport最初的结果是128，而不是$16+6\sqrt{6}$，后者是由Ennola[15]证明的。我们在这里的证明与文献[15]的有所不同。

第 5 章

虚二次域的 Gauss 类数猜想

本章中我们要叙述虚二次域的 Gauss 类数猜想是如何解决的。在第一节中，首先证明类数 1 的虚二次域除 Gauss 所知道的九个以外，至多还有另一个，并且这个可能的例外域的判别式的绝对值大于 $e^{2.2\times10^7}$，前者是 30 年代由 Heilbronn 与 Linfoot[31] 证明的，后者是 1965 年由 H. Stark[95] 证明的。在第一节的最后证明前面所说的例外域不存在，即 Gauss 关于只存在九个类数 1 的虚二次域的猜想是正确的，这是 1966 年由 A. Baker[3] 与 H. Stark[96] 独立地证明的。1952 年时，K. Heegner 在一篇论文[29]中也给出了证明，但证明中用到了 Weber 的一些还没有被证明的断言，因此当时认为他的证明不对。在 1966 年以后的几年中，H. Stark[97]，[98] 等人补出了 Heegner 证明中的漏洞。这样，虚二次域类数 1 猜想的解决，一般称之为 Heegner-Baker-Stark 定理。不但如此，Heegner 的想法，后来在椭圆曲线的研究中起了很重要的作用，被用来找出具有某种特殊性质的椭圆曲线，即用来验证椭圆曲线的著名的 BSD 猜想的有关断言。在虚二次 Gauss 类数问题的解决中，非常关键的一步，是 D. Goldfeld 于 1976 年的一篇影响深远的论文[22]，其中他把虚二次 Gauss 类数问题的解决，归结为找到一条其 L 函数在 $s=1$ 处有一个至少为三阶的零点的椭圆模曲线(对实二次域也有类似结论)。后一个任务，是 B. Gross 与 D. Zagier 花了七年的努力之后，于 1983 年完成的[23]。所以这一解决，称之为 Goldfeld-Gross-Zagier 定理，因此我们在第 2 节中，首先介绍椭圆曲线的理论，特别是 BSD 猜想，然后讨论一条具有所需性质的椭圆曲线。在第 3 节中，我们叙述 Goldfeld-Gross-

Zagier 定理的证明。特别还要指出在第二节与第三节中用到了模形式理论(包括整权的与半整权的)。

§1 类数 1 的虚二次域的最后确定

本节中,我们要给出下列定理的完整证明。

Heegner-Baker-Stark 定理 正好存在九个类数 1 的虚二次域,它们的判别式分别是 -3, -4, -7, -8, -11, -19, -43, -67, -163。

在 1972 年左右, Baker-Stark 还证明了正好存在十八个类数为 2 的虚二次域,它们的判别式是 -15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -116, -123, -148, -187, -235, -267, -403, -427。他们的这一结果的证明,这里不再叙述了,因为 Goldfeld-Gross-Zagier 定理已经彻底解决了虚二次域的类数问题。

1.1 例外域的讨论(一)

在本小节和下一小节中,我们将证明类数 1 的虚二次域除上述列举的九个以外,至多可能还有一个例外域,并且这个可能的例外域的判别式的绝对值大于 $e^{2.2\times10^7}$。

首先在第四章的定理 1.3 中,取 $\varepsilon=0.07$, 则由类数公式可知,虚二次域 $K=Q(\sqrt{d})$ 的判别式 d 满足 $|d|>e^{\frac{1}{\varepsilon}}>1.61\times10^6$ 时,除去至多可能有一个例外域, K 的类数

$$h_K>\min\left\{\frac{\sqrt{|d|}}{8\pi\log|d|},\ \frac{0.98|d|^{0.43}}{\pi}\right\}, \tag{5.1}$$

这个不等式的右边大于 5, 若 $|d|>3.6\times10^6$。因此我们证明了下面的引理。

引理 1.1 当负的基本判别式 d 的绝对值大于 3.6×10^6 时,除去至多可能有一个例外域,虚二次域 $K=Q(\sqrt{d})$ 的类数 $h_K\geqslant 6$。

利用 Buell 所计算的，$-4\times10^6<d\leqslant-3$ 时，$K=Q(\sqrt{d})$ 的类数表可知：当 $-4\times10^6<d\leqslant-3$ 时，如 $h_K\leqslant5$，则 $|d|<3000$。我们就有了下列的表(见表 1)：

表 1

h	所有使 $h_K=h$，$K=Q(\sqrt{-d})$ 的 d，$3\leqslant d<4\times10^6$							
1	3	4	7	8	11	19	43	67
	163							
2	15	20	24	35	40	51	52	88
	91	115	123	148	187	232	235	267
	403	427						
3	23	31	59	83	107	139	211	283
	307	331	379	499	547	643	883	907
4	39	55	56	68	84	120	132	136
	155	168	184	195	203	219	228	259
	280	291	292	312	323	328	340	355
	372	388	408	435	483	520	532	555
	568	595	627	667	708	715	723	760
	763	772	795	955	1, 003	1, 012	1, 027	1, 227
	1, 243	1, 387	1, 411	1, 435	1, 507	1, 555		
5	47	79	103	127	131	179	227	347
	443	523	571	619	683	691	739	787
	947	1, 051	1, 123	1, 723	1, 747	1, 867	2, 203	2, 347
	2, 683							

这样我们得到定理 1.1。

定理 1.1 类数小于等于 5 的虚二次域 $K=Q(\sqrt{d})$，除去上述表中所列的 122 个以外，至多还有一个可能的例外域，且这个例外域的判别式小于 -4×10^6。

1.2 例外域的讨论(二)

本小节中，我们来证明下面的引理。

引理 1.2 (H. Stark[95]) 类数 1 的虚二次域 $K=Q(\sqrt{d})$

除去上述所列的九个以外，至多还可能有一个例外域，且这个例外域的判别式的绝对值是一个素数 p，$p>e^{2.2\times10^7}$。

证明　设 $K=Q(\sqrt{d})$ 为由引理1.1中所说的例外域。由定理1.1可知 $|d|>4\times10^6$。再由第二章引理2.3可知 $|d|$ 是一个素数 p，且 $p\equiv3\pmod 4$，即有 $d=-p$。于是 $p>4\times10^6$。

由第三章(3.117)，定理2.3(3.130)，并取 $k=1$，即有

$$\zeta(s)L(s,\chi_d)=\zeta(2s)+p^{\frac{1}{2}-s}2^{s-1}\sqrt{\pi}\frac{\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)}\zeta(2s-1)$$

$$+\frac{2^{s+3/2}\pi^s}{\Gamma(s)}p^{\frac{1}{4}-\frac{s}{2}}\sum_{u=1}^{\infty}(-1)^u u^{s-\frac{1}{2}}K_{s-\frac{1}{2}}(\pi u\sqrt{p})\sum_{1\leqslant n|u}n^{1-2s},\tag{5.2}$$

并由(3.130)以下的叙述(以及附注)可知，(5.2)的成立范围是

$$\sigma=\mathrm{Re}s\geqslant\frac{1}{2},\quad s\neq\frac{1}{2},$$

K_ν 是 Bessel 函数。

利用 $\zeta(s)$ 的函数方程，由(5.2)可得：

$$\zeta(s)L(s,\chi_d)=\zeta(2s)+\left(\frac{4\pi^2}{p}\right)^{s-\frac{1}{2}}\frac{\Gamma(1-s)}{\Gamma(s)}\zeta(2-2s)+g(s),\tag{5.3}$$

$$g(s)=\frac{2^{\frac{3}{2}+s}\pi^s}{\Gamma(s)}p^{\frac{1}{4}-\frac{s}{2}}\sum_{u=1}^{\infty}(-1)^u u^{s-\frac{1}{2}}K_{s-\frac{1}{2}}(\pi u\sqrt{p})\sum_{1<n|u}n^{1-2s},\tag{5.4}$$

注意(5.3)，(5.4)的成立范围分别是

$$\sigma=\mathrm{Re}s\geqslant\frac{1}{2},\quad s\neq\frac{1}{2};\quad \mathrm{Re}s>0.$$

令 $s=\frac{1}{2}+i\alpha$，$\alpha>0$ 且 $\frac{1}{2}+i\alpha$ 为 $\zeta(s)$ 的零点。则由(5.3)可得

$$\left(\frac{p}{4\pi^2}\right)^{i\alpha}=-\frac{\zeta(1-2i\alpha)}{\zeta(1+2i\alpha)}\frac{\Gamma\left(\frac{1}{2}-i\alpha\right)}{\Gamma\left(\frac{1}{2}+i\alpha\right)}-\frac{g\left(\frac{1}{2}+i\alpha\right)}{\zeta(1+2i\alpha)}.\tag{5.5}$$

今有(参见文献[20] p.959, 8.)

$$K_{i\alpha}(\pi u\sqrt{p})=\frac{\sqrt{\frac{\pi}{2}}(\pi u\sqrt{p})^{i\alpha}}{\Gamma\left(\frac{1}{2}+i\alpha\right)}e^{-\pi u\sqrt{p}}$$

$$\times\int_0^\infty e^{-\pi u\sqrt{p}v}v^{-\frac{1}{2}+i\alpha}\left(1+\frac{v}{2}\right)^{-\frac{1}{2}+i\alpha}dv,$$

从而

$$|K_{i\alpha}(\pi u\sqrt{p})|\leqslant\frac{\sqrt{\frac{\pi}{2}}e^{-\pi u\sqrt{p}}}{\left|\Gamma\left(\frac{1}{2}+i\alpha\right)\right|}\int_0^\infty\frac{e^{-\pi u\sqrt{p}v}dv}{\sqrt{v\left(1+\frac{v}{2}\right)}}$$

$$\leqslant\frac{\sqrt{\frac{\pi}{2}}e^{-\pi u\sqrt{p}}}{\left|\Gamma\left(\frac{1}{2}+i\alpha\right)\right|}\int_0^\infty\frac{e^{-\pi u\sqrt{p}v}}{\sqrt{v}}dv,$$

但最后的积分为

$$\frac{\Gamma\left(\frac{1}{2}\right)}{\sqrt{\pi u\sqrt{p}}}=\frac{1}{\sqrt{u\sqrt{p}}}.$$

由此及(5.4)即有

$$\left|g\left(\frac{1}{2}+i\alpha\right)\right|\leqslant\frac{\sqrt{8}\,\pi p^{-0.25}}{\left|\Gamma\left(\frac{1}{2}+i\alpha\right)\right|^2}\sum_{u=1}^\infty\frac{\tau(u)}{\sqrt{u}}e^{-\pi u\sqrt{p}},\tag{5.6}$$

这里 $\tau(u)$是 u 的正因子的个数。

容易由 $\tau(u)$的积性得到:

$$\tau(u)\leqslant\sqrt{3u},\ u\geqslant1.\tag{5.7}$$

再用(参考文献[20]p.937, 8.332, 2)

$$\left|\Gamma\left(\frac{1}{2}+i\alpha\right)\right|^2=\frac{2\pi}{e^{\pi\alpha}+e^{-\pi\alpha}},\tag{5.8}$$

由(5.6)、(5.8)可得

$$\left|g\left(\frac{1}{2}+i\alpha\right)\right|\leqslant\frac{\sqrt{6}\,p^{0.25}e^{-\pi\sqrt{p}}(e^{\alpha\pi}+e^{-\alpha\pi})}{1-e^{-\pi\sqrt{p}}}$$

$$<10^{-100},\ 如\ p>10^4,\ 0<\alpha<22,\tag{5.9}$$

以下以 θ 表示一个复数(也可能是一个实数), 并且不一定每

一次出现时都相同，但总是满足$|\theta|\leqslant 1$。

今取$\alpha=\alpha_1, \alpha_2$，使$s_j=\frac{1}{2}+i\alpha_j (j=1, 2)$为$\zeta(s)$在$\mathrm{Re}\, s=\frac{1}{2}$，$\mathrm{Im}\, s>0$上的最初的两个零点。对此我们有（见H.Stark [95]）

$$\left.\begin{aligned}
&\alpha_1=14.134725141734693790457+10^{-21}\theta,\\
&\alpha_2=21.022039638771554992628+10^{-21}\theta,\\
&\frac{1}{\pi}\arg\zeta(2s_1)=-0.108452737083095+10^{-10}\theta(\mathrm{mod}\,2),\\
&\frac{1}{\pi}\arg\zeta(2s_2)=0.067103865503910+10^{-10}\theta(\mathrm{mod}\,2),\\
&|\zeta(2s_1)|=1.94875731381740+10^{-10}\theta,\\
&|\zeta(2s_2)|=0.830962021546955+10^{-10}\theta,\\
&\frac{1}{\pi}\arg\Gamma(s_1)=7.418512651985173+2\times 10^{-13}\theta,\\
&\frac{1}{\pi}\arg\Gamma(s_2)=13.688619111000235+2\times 10^{-13}\theta,\\
&\frac{\alpha_2}{\alpha_1}=1.4872620038928 90048+10^{-18}\theta.
\end{aligned}\right\}\tag{5.10}$$

这样，由(5.5)、(5.9)及$|\zeta(2s_j)|>\frac{1}{2}$，可得

$$\left(\frac{p}{4\pi^2}\right)^{i\alpha_j}=-\frac{\zeta(1-2i\alpha_j)}{\zeta(1+2i\alpha_j)}\cdot\frac{\Gamma\left(\frac{1}{2}-i\alpha_j\right)}{\Gamma\left(\frac{1}{2}+i\alpha_j\right)}(1+2\times 10^{-19}\theta),\ j=1, 2. \tag{5.11}$$

(5.11)两边取幅角，即得

$$\alpha_j\log\frac{p}{4\pi^2}=a_j+2\pi x_j+3\times 10^{-19}\theta,\ j=1, 2. \tag{5.12}$$

这里x_j为有理整数，而且$x_j>0$，以及

$$a_j \equiv \pi - 2\arg\zeta(2s_j) - 2\arg\Gamma(s_j) \pmod{2\pi},\ 0 \leqslant a_j < 2\pi.$$

由上述所列的 α_j 等的数值，可算得

$$\frac{a_1}{2\pi} \equiv 0.189940085097922 + 1.002\times10^{-19}\theta \pmod 1,$$

$$\frac{a_2}{2\pi} \equiv 0.744277023495855 + 1.002\times10^{-19}\theta \pmod 1,$$

由于上面的这些数都在 0 与 1 之间，所以这两个同余式实际上是等式。从而可以算出

$$\begin{aligned} a_0 &\overset{\text{def}}{=\!=} \frac{\alpha_2}{\alpha_1}\left(\frac{a_1}{2\pi}\right) - \frac{a_2}{2\pi} \\ &= -0.461786351913533 + 3\times10^{-10}\theta = a + 0.4\times10^{-9}\theta, \end{aligned}$$

$$a = -0.461786352, \tag{5.13}$$

由(5.12)消去 $\log\frac{p}{4\pi^2}$，并解出 x_2，可得

$$x_2 = \frac{\alpha_2}{\alpha_1}x_1 + a_0 + 10^{-18}\theta = \frac{\alpha_2}{\alpha_1}x_1 + a + 0.5\times10^{-9}\theta, \tag{5.14}$$

则有

$$3.999999660 = \frac{3\alpha_2}{\alpha_1} + a + 0.5\times10^{-9}\theta, \tag{5.15}$$

把(5.14)与(5.15)两式相减，可得

$$x_2 - 4 = \frac{\alpha_2}{\alpha_1}(x_1 - 3) - b + 10^{-9}\theta,\ b = 0.000000340, \tag{5.16}$$

置

$$\begin{aligned} &p_1 = 83532765,\quad p_2 = 12832922,\\ &q_1 = 56165467,\quad q_2 = 8628555, \end{aligned} \tag{5.17}$$

则有 $p_1q_2 - p_2q_1 = 1$，故 p_1 与 q_1 互素，且有

$$\left|\frac{\alpha_2}{\alpha_1} - \frac{p_1}{q_1}\right| < 2.3\times10^{-16}. \tag{5.18}$$

令有理整数 Q 与 R 满足

$$0 \leqslant R < q_1,\quad Q + \frac{R}{q_1} = \frac{p_1}{q_1}(x_1 - 3), \tag{5.19}$$

则由(5.16)与(5.18)有：

$$x_2 - Q - 4 = \left(\frac{\alpha_2}{\alpha_1} - \frac{p_1}{q_1}\right)(x_1 - 3) + \frac{R}{q_1} - b + 10^{-9}\theta. \tag{5.20}$$

如 $x_1 \leqslant 5.1\times10^7$，则由(5.18)有

$$\left|\left(\frac{\alpha_2}{\alpha_1} - \frac{p_1}{q_1}\right)(x_1 - 3)\right| < 12\times10^{-9}, \tag{5.21}$$

从而，由 $x_1 \leqslant 5.1\times10^7$，可从(5.20)与(5.21)得出

$$|x_2 - Q - 4| < 12\times10^{-9} + (1 - 34\times10^{-9}) + 10^{-9} < 1, \tag{5.22}$$

其中还用到(5.16)与(5.19)。另一方面，由(5.17)和(5.16)可得

$$\frac{18}{q_1} < 321\times10^{-9} < b = 34\times10^{-9} < 356\times10^{-9} < \frac{20}{q_1},$$

从而，当 $x_1 \leqslant 5.1\times10^7$ 且 $R \neq 19$ 时，可有

$$|x_2 - Q - 4| \geqslant \left|\frac{R}{q_1} - b\right| - \left|\left(\frac{\alpha_2}{\alpha_1} - \frac{p_1}{q_1}\right)(x_1 - 3)\right| - 10^{-9}$$
$$> 16\times10^{-9} - 12\times10^{-9} - 10^{-9} > 0,$$

这与(5.22)矛盾，因为 $x_2 - Q - 4$ 是有理整数。所以 $x_1 \leqslant 5.1\times10^7$ 时，一定有 $R = 19$，但当 $R = 19$ 时，由(5.19)有

$$19 \equiv p_1(x_1 - 3) \pmod{q_1},$$

解这个同余方程，可得

$$x_1 - 3 \equiv 51611611 \pmod{q_1},$$

这样再结合 $x_1 > 0$ 及(5.17)可知，不可能有 $x_1 \leqslant 5.1\times10^7$。

因此，我们证明了一定有 $x_1 > 5.1\times10^7$。从而由(5.12)即知

$$p > e^{2.2\times10^7}.$$

引理证毕。

1.3 类数1的虚二次域的决定

本小节中，我们给出 Heegner-Baker-Stark 定理的证明，即来证明以上所说的例外域不存在。所用的方法，综合了 H.Stark 和 A.Baker 的方法。

由上一小节知道，可设这个可能的类数1的例外域

$$K=Q(\sqrt{-q}),$$

其中 q 是一个有理素数，$q\equiv 3(\mathrm{mod}\,4)$，且 $q>e^{2.2\times10^7}$。

在第三章引理2.1中，取 $d=-q$，k 为任一个正的与 q 互素的至少具有两个不同素因子的基本判别式，则有

$$\left|L(1,\ \chi_k)L(1,\ \chi_k\chi_d)-\frac{\pi^2}{6}\prod_{p\mid k}(1-p^{-2})\right|$$

$$\leqslant\frac{4\pi}{\sqrt{q}}\ \frac{e^{-\pi\sqrt{q}/k}}{1-e^{-\pi\sqrt{q}/k}},\qquad(5.23)$$

这里 $\chi_k(*)=\left(\frac{k}{*}\right)$，$\chi_d(*)=\left(\frac{d}{*}\right)$为 Kronecker 符号，$p$ 表有理素数。(5.23)的证明，还用到第三章的定理2.3的结论

$$\tilde{L}(1,\ \chi_k)=L(1,\ \chi_k)L(1,\ \chi_k\chi_d).$$

由 $g.c.d.(k,\ d)=1$，kd为一个负的基本判别式，$\chi_k\chi_d=\chi_{kd}$ 是 Kronecker 符号$\left(\frac{kd}{*}\right)$。由类数公式，有

$$\sqrt{k}L(1,\ \chi_k)=2h(k)\log\varepsilon_k,\quad \sqrt{kq}L(1,\ \chi_{kd})=\pi h(kd),\tag{5.24}$$

这里 ε_k 为 $Q(\sqrt{k})$ 的基本单位，$h(k)$ 与 $h(kd)$ 分别是二次域 $Q(\sqrt{k})$与$Q(\sqrt{kd})$的类数。

这样，由(5.23)与(5.24)可得

$$\left|h(k)h(kd)\log\varepsilon_k-\frac{\pi k\sqrt{q}}{12}\prod_{p\mid k}(1-p^{-2})\right|\leqslant\frac{2ke^{-\pi\sqrt{q}/k}}{1-e^{-\pi\sqrt{q}/k}},\tag{5.25}$$

在(5.25)中，分别取 $k=12$ 与 24，即得

$$\left|h(-12q)\log(2+\sqrt{3})-\frac{2}{3}\pi\sqrt{q}\right|\leqslant\frac{24e^{-\frac{\pi\sqrt{q}}{12}}}{1-e^{-\frac{\pi\sqrt{q}}{12}}},\quad(5.26)$$

$$\left|h(-24q)\log(5+2\sqrt{6})-\frac{4}{3}\pi\sqrt{q}\right|\leqslant\frac{48e^{-\frac{\pi\sqrt{q}}{24}}}{1-e^{-\frac{\pi\sqrt{q}}{24}}}.\tag{5.27}$$

由(5.26)、(5.27)及 $q>e^{2.2\times 10^7}$，即有

$$|h(-24q)\log(5+2\sqrt{6})-2h(-12q)\log(2+\sqrt{3})|$$

$$<49e^{-\frac{\pi\sqrt{q}}{24}}, \tag{5.28}$$

$$h(-12q),\ h(-24q)<2\sqrt{q}. \tag{5.29}$$

我们要用 A.Baker[4] 的一个有关结果（该书 $p.6$，定理 2，并取 $n=2$）。

定理 1.2 设代数数 α_1，α_2 的高分别小于等于 A_1，A_2；β_1，β_2 为有理整数，它们的绝对值小于等于 B。如果 A_1，A_2，$B\geqslant 4$，且对数线性型

$$\Lambda=\beta_1\log\alpha_1+\beta_2\log\alpha_2\neq 0,$$

（对数取主值），则有

$$|\Lambda|>B^{-C(\log A_1)(\log A_2)(\log\log A_2)},$$

这里 $C=(32m)^{400}$，其中 m 是 $Q(\alpha_1,\alpha_2)$ 的次数，即

$$m=[Q(\alpha_1,\ \alpha_2):Q].$$

由于 $2+\sqrt{3}$，$5+2\sqrt{6}$ 分别为下列二个有理整系数二次方程的根：

$$z^2-4z+1=0,\ z^2-10z+1=0,$$

故 $2+\sqrt{3}$ 与 $5+2\sqrt{6}$ 的高分别为 4 与 10。又由 genus 理论可知 $h(-12q)$ 与 $h(-24q)$ 均为 4 的倍数，又

$$[Q(2+\sqrt{3},\ 5+2\sqrt{6}):Q]=4.$$

这样，由定理 1.2、(5.28) 和(5.29)，可得

$$49e^{-\frac{\pi\sqrt{q}}{24}}>(2\sqrt{q})^{-128^{400}(\log 4)(\log 10)(\log\log 4)},$$

取对数，即有（用 $q>e^{2.2\times 10^7}$）

$$e^{1.1\times 10^7}\Big(1-\frac{12}{\pi}\times 128^{400}(\log 4)(\log 10)(\log\log 4)$$

$$\times 2.2\times 10^7\times e^{-1.1\times 10^7}\Big)$$

$$<\frac{24}{\pi}(128^{400}(\log 4)(\log 10)(\log\log 4)(\log 2)$$

$$+\log 49),$$

由此可得

$$e^{10^7} < e^{2000},$$

这不可能，这就证明了例外域不存在。

这样我们已完全证明了 Heegner-Baker-Stark 定理，即完全证明了 Gauss 关于只有九个类数1的虚二次域的著名猜想。

§2 椭圆曲线与模形式

我们在本节中，概要地介绍椭圆曲线的有关理论，特别是椭圆曲线的 L 函数及其 BSD 猜想，最后对一条具体的椭圆曲线进行细致的分析。一般来说，我们不给出证明，有关的详细内容，可以参考下列的三本书：

(1) J. Silverman: The Arithmetic of Elliptic Curves, GTM 106. Springer-Verlag, 1986.

(2) D. Husemöller: Elliptic Curves, GTM 111. Springer-Verlag. 1987.

(3) N. Koblitz: Introduction to Elliptic Curves and Modular Forms. GTM 97. Springer-Verlag. 1984.

2.1 椭圆曲线理论概要

(I) 基本定义

设 K 为一个域，$\overline{K}$ 是 K 的一个固定的代数闭包。

$\overline{K}$ 中一条亏格(genus)为1的非奇异的射影曲线 E 以及 E 上的一个点 O，即这样的一对 (E, O)，我们称之为一条椭圆曲线，通常只记为 E，而点 O 作自然的理解（一般情况下会适当地指出）。如果 E 在域 K 上有定义，且 $O \in E(K)$，这里 $E(K)$ 表示射影曲线 E 上所有坐标取自 K 的点的全体，则称 (E, O) 定义在 K 上，并记为 E/K 或 E_K。

在同构的意义下，椭圆曲线 E_K 可以理解为由下列非奇异 Weierstrass 方程(齐次坐标)

$$E: \ y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \qquad (5.30)$$

在 $P^2(K)$ 中定义的轨迹，并且 $O=[0,1,0]$，这里 $a_1, \cdots, a_6 \in K$；而非奇异的意义是 $\Delta \neq 0$，Δ 是 E 的判别式，它可如下决定之：命

$$b_2 = a_1^2 + 4a_2,\ b_4 = a_1a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \tag{5.31}$$

则

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{5.32}$$

我们指出，有恒等式

$$4b_8 = b_2b_6 - b_4^2. \tag{5.33}$$

如果用非齐次坐标，Weierstrass 方程便是

$$E:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{5.34}$$

点 O 成为无穷远点

再命

$$c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \tag{5.35}$$

$$j = j(E) = \frac{c_4^3}{\Delta}(注意\ \Delta \neq 0), \tag{5.36}$$

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}. \tag{5.37}$$

下列形式的映射，称为 E 的允许映射：

$$x = u^2\tilde{x} + r,\qquad y = u^3\tilde{y} + su^2\tilde{x} + t, \tag{5.38}$$

其中 $u, r, s, t \in K$，且 u 可逆，即 $u \neq 0$。它使点 $O=[0,1,0]$ 不动。

在允许映射下，E 变为另一条与之同构的椭圆曲线 $\tilde{E}$：

$$\tilde{E}:\ \tilde{y}^2 + \tilde{a}_1\tilde{x}\tilde{y} + \tilde{a}_3\tilde{y} = \tilde{x}^3 + \tilde{a}_2\tilde{x}^2 + \tilde{a}_4\tilde{x} + \tilde{a}_6, \tag{5.39}$$

在允许映射(5.38)下，(5.39)的有关量的变化是

$$u\tilde{a}_1 = a_1 + 2s,$$
$$u^2\tilde{a}_2 = a_2 - sa_1 + 3r - s^2,$$
$$u^3\tilde{a}_3 = a_3 + ra_1 + 2t,$$
$$u^4\tilde{a}_4 = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,$$
$$u^6\tilde{a}_6 = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,$$
$$u^2\tilde{b}_2 = b_2 + 12r,$$
$$u^4\tilde{b}_4 = b_4 + rb_2 + 6r^2,$$

$$u^6\tilde{b}_6 = b_6 + 2rb_4 + r^2b_2 + 4r^3,$$
$$u^8\tilde{b}_8 = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4,$$
$$u^4\tilde{c}_4 = c_4,$$
$$u^6\tilde{c}_6 = c_6,$$
$$u^{12}\tilde{\Delta} = \Delta,$$
$$\tilde{j} = j,$$
$$u^{-1}\tilde{\omega} = \omega.$$

反之，同构的椭圆曲线E与$\tilde{E}$之间的同构映射，当E与$\tilde{E}$均采用Weierstrass方程，且点O也均采用[0, 1, 0]时，必是允许映射(5.38)。

这样就得到引理2.1。

引理 2.1 j与ω都是在同构下不变的，注意所谓ω不变的意思是只差一个不为零的常数倍。

j称为E的j-不变量，ω称为E的不变微分。

由(5.32)、(5.33)和(5.35)可得

$$12^3\Delta = c_4^3 - c_6^2. \tag{5.40}$$

所以，我们有

$$j = \frac{(12c_4)^3}{c_4^3 - c_6^2}, \text{ 如 } \mathrm{ch}(K) \neq 2,\ 3. \tag{5.41}$$

引理 2.2 两条椭圆曲线在$\overline{K}$上同构当且仅当它们具有相同的j-不变量。

证明 略。

如$\mathrm{ch}(K) \neq 2$，则在允许映射

$$x \mapsto x, \quad y \mapsto y + \frac{1}{2}(a_1x + a_3) \tag{5.42}$$

F，E的Weierstrass方程成为下列形式：

$$E: \ 4y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{5.43}$$

其不变微分$\omega = \dfrac{dx}{2y}$。

如$\mathrm{ch}(K) \neq 2,\ 3$，则对方程(5.43)再作允许映射：

$$x \mapsto x + \frac{b_2}{12},\ y \mapsto y, \tag{5.44}$$

则 E 的 Weierstrass 方程成为下列形式：

$$E: \ y^2 = x^3 - \frac{c_4}{48} x - \frac{c_6}{864}, \tag{5.45}$$

它的判别式 $\Delta = D(f)$，即为三次多项式

$$f(x) = x^3 - \frac{c_4}{48} x - \frac{c_6}{864} \tag{5.46}$$

的判别式，因为 $\Delta \neq 0$，所以 $f(x)$ 在 $\overline{K}$ 中有三个不同的根。

另外可知，椭圆曲线(5.45)的不变微分 $\omega = \frac{dx}{2y}$。

以下三条椭圆曲线均在任意域中定义：

(1) $E: \ y^2 = x^3 + a$，其 j—不变量 $j = 0$，$6a \neq 0$；

(2) $E: \ y^2 = x^3 + ax$，其 j—不变量 $j = 12^3 = 1728$，如 $2a \neq 0$；

(3) $E: \ y^2 + xy = x^3 - \frac{36}{j - 1728} x - \frac{1}{j - 1728}$，其 j—不变量 $= j$，如 $j \neq 0, 1728$。

(I) 群运算(Mordell-Weil 群)

引理 2.3 每条椭圆曲线 (E, O) 均构成一个 Abel 群，这个群的恒等元是 O，当 E 由 Weierstrass 方程

$$E: \ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

给出时，这个群的运算 $\oplus$，如下定义：

对 $P_1(x_1, y_1)$，$P_2(x_2, y_2) \in E$，

$$P_3(x_3, y_3) = P_1(x_1, y_1) \oplus P_2(x_2, y_2) \in E,$$

有：

(1) $P_3(x_3, y_3) = O$ 当且仅当 $x_2 = x_1$，$y_2 = -y_1 - a_1 x_1 - a_3$，一般地，对 $P_0(x_0, y_0) \in E$，P_0 的逆是

$$-P_0 = (x_0, \ -y_0 - a_1 x_0 - a_3);$$

(2) 当 $x_2 = x_1$ 与 $y_2 = -y_1 - a_1 x_1 - x_3$ 不同时成立时，命

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}, \text{ 如 } x_2 \neq x_1;$$

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3},$$

$$\nu=\frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3},\quad 如\ x_2=x_1。$$

(注意，在所给的条件下，当 $x_2=x_1$ 时，必然有 $y_2=y_1$)。则

$$x_3=\lambda^2+a_1\lambda-a_2-x_1-x_2,\ y_3=-(\lambda+a_1)x_3-\nu-a_3;$$

(3) 当 $P_1\neq\pm P_2$ 时，

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2+a_1\left(\frac{y_2-y_1}{x_2-x_1}\right)-a_2-x_1-x_2;$$

(4) 当 $P_1=P_2=P=P(x,y)\in E$ 时，$P_3(x_3,y_3)=P_3=P_1\oplus P_2=P\oplus P$，记为 $P_3=2P$，并有

$$x_3=\frac{x^4-b_4x^2-2b_6x-b_8}{4x^3+b_2x^2+2b_4x+b_6}.$$

我们可以把上述群运算用以下两图显示：

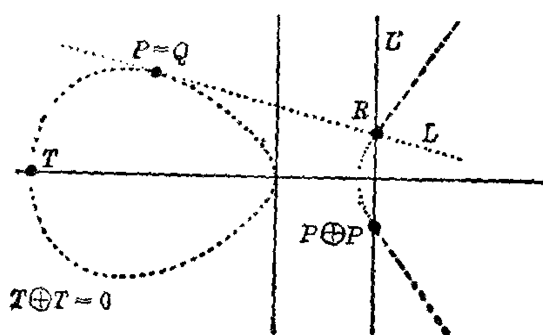


图 1

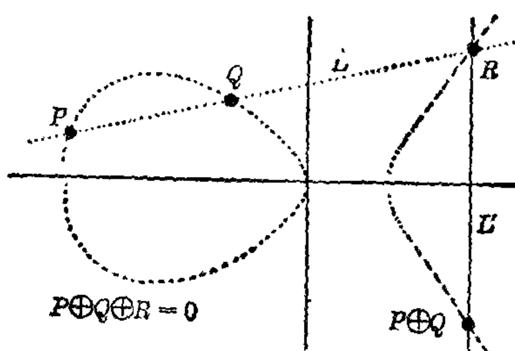


图 2

这两个图的解释是：连结 E 的两个点 P 与 Q 的直线(当 $P=Q$ 时，为过该点的切线)与 E 交于第三点 R，连结 R 与 O 的直线与 E 交于另一个点，而最后的这个点定义为 $P\oplus Q$。

定理 2.1(Mordell-Weil) 如 K 是一个数域，E/K 为一条椭圆曲线。则如上构作的群 $E_K=E(K)$ 是一个有限秩的 Abel 群，即

$$E(K)\cong E_{tor}(K)\times Z^r,$$

这里 r 是 $E(K)$ 的秩，$E_{tor}(K)$ 是 $E(K)$ 的 torsion 子群，即由 $E(K)$ 的所有有限阶元素组成的子群，它是一个有限群。

定理 2.2(B.Mazur)

(1) 设 K 为一个数域，p 为一个有理素数。那么存在一个常

数 $N=N(\mathbb{K}, p)$ 使得对所有的椭圆曲线 $E/\mathbb{K}$，均有：

$$|E(\mathbb{K})_p|\leqslant p^N,$$

这里 $E(\mathbb{K})_p$ 表示 $E(\mathbb{K})$ 的 p 一部分。

(2) 设 $E/\mathbb{Q}$ 为一条椭圆曲线，则 torsion 子群 $E_{tor}(\mathbb{Q})$ 必为下列 15 种群之一：

$$\mathbb{Z}/N\mathbb{Z}: \ 1\leqslant N\leqslant 10 \text{ 或 } N=12;$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2N\mathbb{Z}: \ 1\leqslant N\leqslant 4.$$

以上两个定理，特别是 Mordell-Weil 定理是椭圆曲线理的基本定理。对数域 $\mathbb{K}$ 上的一条椭圆曲线 $E/\mathbb{K}$，群 $E(\mathbb{K})$ 称为 Mordell-Weil 群，当然也可以对一般域这样称呼。Mordell-Weil 定理说明，对数域上的一条椭圆曲线 E，它的 Mordell-Weil 群是有限秩的。从而有下面的重要定义。

定义 2.1 对数域 $\mathbb{K}$ 上一条椭圆曲线 $E/\mathbb{K}$，定理 2.1 中所确定的非负整数 r，称为 $E/\mathbb{K}$ 的秩，记为 $\operatorname{rank}(E/\mathbb{K})=r$。

对数域 $\mathbb{K}$ 上一条给定的椭圆曲线 $E/\mathbb{K}$，算出它的秩，是一个重要的工作。特别是有理数域 $\mathbb{Q}$ 上的椭圆曲线 $E/\mathbb{Q}$，这方面已有很多工作，已经算出有 $0\leqslant r\leqslant 14$ 的 $E/\mathbb{Q}$。一般猜想有 r 任意大的 $E/\mathbb{Q}$。

如果 Weierstrass 方程

$$E: \ y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \tag{5.47}$$

是奇异的，即其判别式 $\Delta=0$，则由 (5.47) 给出的曲线 E 上有一个唯一的奇点 S：当 $c_4\neq 0$ 时，S 是一个结点(Node)；当 $c_4=0$ 时，S 是一个尖点(Cusp)。令 E_{ns} 是 (5.47) 给出的曲线 E 的非奇异部分(当然还要附上无穷远点 O)。那么由上述引理 2.3 所定义的运算⊕，仍使 E_{ns} 成为一个 Abel 群。并可区分为下列的几种情况：

(a) 设 $c_4\neq 0$，即 S 为一个结点(Node)时，令 E 在 S 处的那两条不同的切线为

$$y=\alpha_ix+\beta_i, \ \alpha_i, \ \beta_i\in\overline{\mathbb{K}}, \ i=1, 2.$$

在映射 $(x, y)\mapsto\dfrac{y-\alpha_1x-\beta_1}{y-\alpha_2x-\beta_2}$ 之下，E_{ns} 同构地映入 $\mathbb{K}^*$，并且：

(a_1)　如有 $\alpha_1\in\mathbb{K}$，则必定也有 $\alpha_2\in\mathbb{K}$，同时还会有

$$E_{\mathrm{ns}}(\mathbb{K})\cong\mathbb{K}^*(\mathbb{K}\text{ 的乘法群}),$$

(a_2)　如果 $\alpha_1\notin\mathbb{K}$(从而也有 $\alpha_2\notin\mathbb{K}$)，则 $\mathbb{Z}=\mathbb{K}(\alpha_1, \alpha_2)$ 是 $\mathbb{K}$ 的一个二次扩域，且有

$$E_{\mathrm{ns}}(\mathbb{K})\cong\{t\in\mathbb{Z}^*|N_{\mathbb{Z}/\mathbb{K}}(t)=1\};$$

(b) 设 $c_4=0$，即 S 为一个尖点(Cusp)时，令 E 在 S 处的那条切线为

$$y=\alpha x+\beta,\ \alpha,\ \beta\in\overline{\mathbb{K}}.$$

在同构映射 $(x, y)\mapsto\dfrac{x-x(s)}{y-\alpha x-\beta}$，($x(S)$ 是 S 的第一个坐标)下，

$$E_{\mathrm{ns}}\cong\mathbb{K}^+(\mathbb{K}\text{ 的加法群})。$$

下面的两个图解释了尖点(Cusp)与结点(Node)。

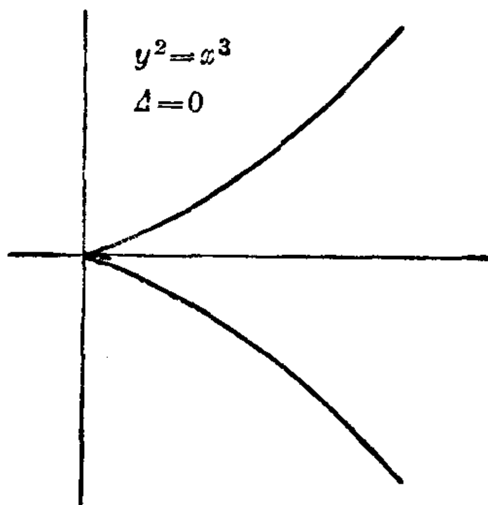


图 3　尖点

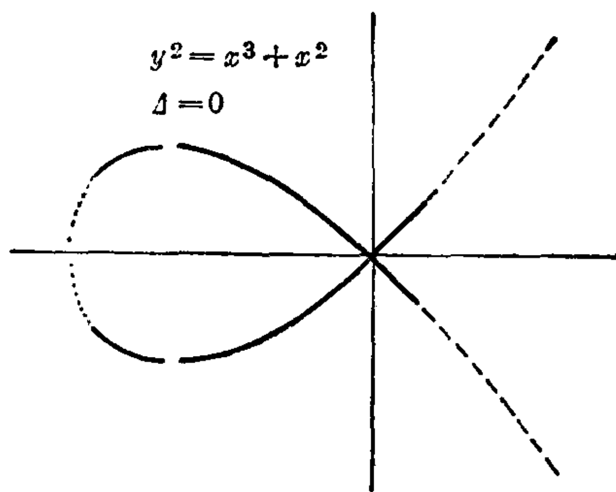


图 4　结点

(Ⅱ)　同态(Isogeny)和复乘(Complex multiplication)

设 E_1，E_2 为两条给定的椭圆曲线，E_1 到 E_2 的一个态射(Morphism)(即处处正则的有理映射)

$$\phi:\ E_1\to E_2$$

如满足 $\phi(0)=0$，就称为 E_1 到 E_2 的一个同态映射，简称为一个同态(isogeny)。如 E_1 与 E_2 之间存在一个同态映射 ϕ，使 $\phi(E_1)$

$\neq \{0\}$，就称 E_1 与 E_2 是同态的(isogenous)。

由于 E_1, E_2 都是群，故由 E_1 到 E_2 的全体同态组成的集合，即

$$\mathrm{Hom}(E_1, E_2) = \{\phi \mid \phi \text{ 为 } E_1 \text{ 到 } E_2 \text{ 的同态}\}$$

是一个群，它的群运算⊕如下定义之：

$$(\phi_1 \oplus \phi_2)(P) = \phi_1(P) \oplus \phi_2(P), \ \forall P \in E_1, \ \phi_1, \ \phi_2 \in \mathrm{Hom}(E_1, E_2).$$

令 $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ 为 E 到自身的全体自同态组成的集合，它是一个环，加法⊕已定义如上，而乘法定义为映射的合成，即

$$(\phi_1\phi_2)(P) = \phi_1(\phi_2(P)), \ \forall P \in E, \ \phi_1, \phi_2 \in \mathrm{End}(E).$$

$\mathrm{End}(E)$ 称为 E 的自同态环。$\mathrm{End}(E)$ 中的可逆元组成了 E 的自同构群，记为 $\mathrm{Aut}(E)$。

当 E_1, E_2, E 是定义在域 $\mathbb{K}$ 上时，我们得到定义在域 $\mathbb{K}$ 上的同态、同态群、自同态环和自同构群，并相应地记为

$$\mathrm{Hom}_{\mathbb{K}}(E_1, E_2), \ \mathrm{End}_{\mathbb{K}}(E), \ \mathrm{Aut}_{\mathbb{K}}(E).$$

定理 2.3　对任一条椭圆曲线 E, $\mathrm{End}(E)$ 是一个特征零的整区，且其对 $\mathbb{Z}$ 的秩至多为 4, 更精密些，$\mathrm{End}(E)$ 只有下列三种可能性：

(1) $\mathrm{End}(E) \cong \mathbb{Z}$；

(2) $\mathrm{End}(E)$ 是 $\mathbb{Q}$ 的一个虚二次扩域中的某个 Order;

(3) $\mathrm{End}(E)$ 是 $\mathbb{Q}$ 的一个四元代数中的某个 Order。

定义 2.2　如对一条椭圆曲线 E 有 $\mathrm{End}(E) \not\cong \mathbb{Z}$, 则称 E 有复乘(Complex Multiplication)。

当 $\mathrm{ch}(\mathbb{K}) = 0$ 时，$\mathrm{End}(E) \otimes \mathbb{Q}$ 不可能是一个四元代数。而当 $\mathbb{K}$ 是有限域时，$\mathrm{End}(E)$ 总是比 $\mathbb{Z}$ 大，并且存在 $\overline{\mathbb{K}}$ 上的椭圆曲线 E, 使 $\mathrm{End}(E)$ 为一非交换的环。关于 $\mathrm{End}(E)$ 的详细而完整的描述见 M. Deuring 的有关论文，其出处可在开头列三本书中找到。

(Ⅳ)　Tate 模

对一个有理整数m，定义椭圆曲线E的一个自同态$[m]$：

$$[m]P=\underbrace{P\oplus\cdots\oplus P}_{m\text{个}},\ \text{如}\ m>0;$$

$$[m]P=[-m](-P),\ \text{如}\ m<0;$$

$$[o]P=O.$$

$[m]$称为用m乘。

设(E,O)是一条椭圆曲线，$m\in\mathbb{Z}$，$m\neq 0$。E的m-torsion子群，记为$E[m]$ 定义为：

$$E[m]=\{P\in E\mid [m]P=O\},$$

即
$$E[m]=\mathrm{Ker}[m].$$

引理 2.4 在上述假定下，我们有如下结论：

(1) 如果$\mathrm{ch}(\mathbb{K})=0$或$m$与$\mathrm{ch}(\mathbb{K})$互素，则有

$$E[m]\cong(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z});$$

(2) 如果$\mathrm{ch}(\mathbb{K})=p$(有理素数)，则有

$$E[p^u]\cong\{O\},\ \forall u=1,2,3,\cdots$$

或

$$E[p^u]\cong\mathbb{Z}/p^u\mathbb{Z},\ \forall u=1,2,3,\cdots.$$

定义 2.3 对一条椭圆曲线E及一个素数$l\in\mathbb{Z}$，E的l-adic Tate 模$T_l(E)$定义为群

$$T_l(E)=\varprojlim_{n} E[l^n],$$

这里的逆极限是相对下列自然映射而取的：

$$E[l^{n+1}]\xrightarrow{[l]}E[l^n].$$

因为每一个$E[l^n]$显然是一个$\mathbb{Z}/l^n\mathbb{Z}$-模，所以$T_l(E)$是一个$\mathbb{Z}_l$-模，这里$\mathbb{Z}_l$是l-adic 整数环。

引理 2.5 作为一个$\mathbb{Z}_l$-模，Tate 模$T_l(E)$有下列结构：

(1) $T_l(E)\cong\mathbb{Z}_l\times\mathbb{Z}_l$，如$l\neq\mathrm{ch}(\mathbb{K})$；

(2) $T_p(E)\cong\{O\}$或$\mathbb{Z}_p$，如$p=\mathrm{ch}(\mathbb{K})$。

(V) ν-约化与导子(Conductor)

设$\mathbb{K}_\nu\supseteq\mathbb{K}$为在$\mathbb{K}$的一个给定的标准离散指数赋值$\nu$下为

完备的局部域，k_ν 为其剩余类域；再设 K_ν 与 k_ν 皆为完全的。设 k_ν 的特征为 p。

经过允许映射后，我们可设椭圆曲线 E 的 Weierstrass 方程

$$E_\nu: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5.48}$$

满足 $\nu(a_i) \geqslant 0$, $i=1, 2, 3, 4, 6$, 并且 $\nu(\Delta)$ 达到极小值。注意这是对一个固定的离散赋值 ν 做的。方程(5.48)称为 E 的 ν-adic 极小 Weierstrass 方程，它代表了 K_ν 上的一条椭圆曲线 E_ν。记剩余类映射为 $a \mapsto \bar{a}$, $\forall a \in K_\nu$ 及 $\nu(a) \geqslant 0$。则我们得到了 k_ν 上的一条三次曲线的 Weierstrass 方程：

$$\bar{E}_\nu: \quad y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6.$$

$\bar{E}_\nu$ 只有下列几种可能：

(1) $\bar{E}_\nu$ 是非奇异的，即 $\bar{E}_\nu$ 是 k_ν 上的一条椭圆曲线，这时称 $\bar{E}_\nu$ 为 E 的一个好约化(good reduction)(或稳定约化)，也称 E 在 ν 处有一个好约化，也称 ν 为 E 的一个好(离散)赋值；

(2) $\bar{E}_\nu$ 不是非奇异的，即 $\bar{E}_\nu$ 不是 k_ν 上的一条椭圆曲线，这时称 $\bar{E}_\nu$ 为 E 的一个坏约化（bad reduction)，也称 E 在 ν 处有一个坏约化，也称 ν 为 E 的一个坏(离散)赋值，这时又可区分为二种子情况：

(2a) $\bar{E}_\nu$ 有一个结点(Node)时，称为乘性约化（或半稳定约化），这时 $\bar{E}_\nu$ 的非奇异部分同构于 $\bar{k}_\nu^*$ (k_ν 的代数闭包 $\bar{k}_\nu$ 的乘法群)的一个子群。并且依据在结点处的切线的斜率是否属于 k_ν 分别称为 Split 乘性约化或非 Split 乘性约化；

(2b) $\bar{E}_\nu$ 有一个尖点(Cusp)时，称为加性约化（或不稳定约化)，这时 $\bar{E}_\nu$ 的非奇异部分同构于 k_ν^+(k_ν 的加法群)。

令

$$f_\nu = \begin{cases} 0, & \text{如} E \text{在} \nu \text{处有一个好约化；} \\ 1, & \text{如} E \text{在} \nu \text{处有一个乘性约化；} \\ 2+\delta_\nu, & \text{如} E \text{在} \nu \text{处有一个加性约化，} \end{cases}$$

这里非负整数 δ_ν 是 Galois 群 $G(\overline{K}_\nu/K_\nu) = \mathrm{Gal}(\overline{K}_\nu/K_\nu)$ 的惯性子群 I_ν 在 Tate 模 $T_l(E)$ 上作用的"野性分歧" (Wildlyramified) 的

一个度量，其中 l 可取为任一个不等于 $p(=\mathrm{ch}(k_v))$ 的有理素数，这个度量是J.P.Serre引进的。当 $p\neq 2, 3$ 时，有 $\delta_v=0$；当 $T_l(E)$ 为"驯性分歧"(Tamelyramified)的 G_{k_v}-模时，$\delta_v=0$。可知，当 $\Delta=\Delta_{E/K}$ 为 E/K 的极小判别式时，$m_v=\mathrm{ord}_v(\Delta)-1-\delta_v$ 是 E 在 v 处极小完备Neron模的特殊纤维的不可约分量的个数。所以 δ_v 的定义极为繁复，上述所述定义的确切含意不能在此详述。可参考本节开头所列的前二本书，那里列有很详细的资料，以及 δ_v 的各种可能性。

f_v 称为 E 在 v 处的导子的幂次。

我们现在可以给出下列重要的关于椭圆曲线的导子的定义：

定义 2.4 设 $\mathbb{K}$ 为一个数域，$E/\mathbb{K}$ 为一条椭圆曲线。$E/\mathbb{K}$ 的导子(Conductor)定义为 $\mathbb{K}$ 的如下的一个整理想：

$$N_{E/\mathbb{K}}=\prod_v \mathfrak{P}_v^{f_v},$$

这里 v 跑过 $\mathbb{K}$ 的所有(彼此不等价的)标准离散指数赋值，$\mathfrak{P}_v$ 为相应于 v 的素理想，f_v 定义如上。

2.2 L-级数与T-W猜想

设 $\mathbb{K}$ 为一个数域，$E/\mathbb{K}$ 为一条椭圆曲线，v 为 $\mathbb{K}$ 的一个离散赋值，可设其为标准指数赋值。置 $q_v=|k_v|$，E 在 v 处的约化记为 $\bar{E}_v$。

对不定元 T，置

$$L_v(T)=\begin{cases}1-a_vT+q_vT^2, & a_v=q_v+1-|\bar{E}_v(k_v)|,\ \text{如}E\text{在}v\text{处有一个好约化；}\\ 1-T, & \text{如}E\text{在}v\text{处有一个Split乘性约化；}\\ 1+T, & \text{如}E\text{在}v\text{处有一个非Split乘性约化；}\\ 1, & \text{如}E\text{在}v\text{处有一个加性约化。}\end{cases}$$

定义 2.5 $E/\mathbb{K}$ 的 L-级数定义为Euler乘积：

$$L_E(s)=L_{E/\mathbb{K}}(s)=\prod_v L_v(q_v^{-s})^{-1},\quad s\in\mathbb{C}, \tag{5.49}$$

这里 v 跑过 $\mathbb{K}$ 的所有(彼此不等价)的离散赋值。由Hasse的一

条定理可知,对好的 ν, 有 $|a_\nu|\leqslant 2\sqrt{q_\nu}$, 于是(5.49)右边的乘积,在 $\mathrm{Re}s>\frac{3}{2}$ 时,是收敛的,从而 $L_E(s)$ 在 $\mathrm{Re}s>\frac{3}{2}$ 时是一个解析函数。

有下列的 Hasse-Weil 猜想。

猜想 5.A 数域 $\mathbb{K}$ 上任一条椭圆曲线 E 的 L-级数 $L_E(s)$ 可以解析开拓到整个 s 平面成为 s 的一个整函数,并且满足

$$\Lambda_{E/\mathbb{K}}(s)\overset{\text{def}}{=\!=}A^{\frac{s}{2}}\Gamma_{\mathbb{K}}(s)L_{E/\mathbb{K}}(s)=w\Lambda_{E/\mathbb{K}}(2-s),$$

这里 $w=\pm 1$, $\Gamma_{\mathbb{K}}(s)=\left(\frac{\Gamma(s)}{(2\pi)^s}\right)^n$, $n=[\mathbb{K}:Q]$, 以及

$$A=A_{E/\mathbb{K}}=\mathbb{N}_{\mathbb{K}/Q}(N_{E/\mathbb{K}})d^2_{\mathbb{K}/Q},$$

其中 $N_{E/\mathbb{K}}$ 为 $E/\mathbb{K}$ 的 Conductor, $d_{\mathbb{K}/Q}$ 为 $\mathbb{K}$ 的绝对判别式, 并且 $\Lambda_{E/\mathbb{K}}(s)$ 也是 s 的整函数。

上述的猜想 **5.A**(Hasse-Weil) 已在许多情况下被证明。

以下,我们取 $\mathbb{K}=Q$。设 $E=E/Q$ 为一条椭圆曲线,

$$L_E(s)=L_{E/Q}(s)$$

为 E 的如上定义的 L-级数或称为 L-函数。E 的导子(Conductor)可取为一个正整数 $N_E=N_{E/Q}$。而有

$$\Lambda_E(s)=N_E^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L_E(s). \tag{5.50}$$

则我们有下列的 Hasse-Weil 猜想。

猜想 5.B 对 Q 上的任一条椭圆曲线 E/Q, 如上定义的函数 $L_E(s)$ 和 $\Lambda_E(s)$ 均可解析开拓到整个 s 平面而成 s 的整函数,且满足函数方程

$$\Lambda_E(s)=w\Lambda_E(2-s),\ w=\pm 1. \tag{5.51}$$

猜想 5.C(Taniyama-Weil) 设 E/Q 是一条椭圆曲线,其导子为 N(正整数),再设

$$L_E(s)=\sum_{n=1}^{\infty}c_n n^{-s}\left(\mathrm{Re}s>\frac{3}{2}\right)$$

为其 L-级数,并令

$$f(\tau)=\sum_{n=1}^{\infty}c_n e^{2\pi i n\tau}(\mathrm{Im}\,\tau>0)$$

为 $L_E(s)$ 的逆 Mellin 变换。则有：

(1) $f(\tau)$是一个 $SL_2(\mathbb{Z})$ 的同余子群 $\Gamma_0(N)$ 的权为 2 的尖点形式，即 $f(\tau)$ 是 τ-上半平面$\mathbb{H}$上的一个解析函数，它在$\mathbb{H}^*/\Gamma_0(N)$ 的每一个尖点处取值(这种取值有特别的定义方式) 均为零，并且满足变换方程：

$$f\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^2f(\tau),\ \forall\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma_0(N),$$

这里

$$\Gamma_0(N)=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle|\begin{matrix}a,\ b,\ c,\ d\in\mathbb{Z};\ ad-bc=1;\\ c\equiv 0(\mathrm{mod}\ N)\end{matrix}\right\},$$

$\mathbb{H}^*=\mathbb{H}\cup P^1(\mathbb{Q})$。

(2) 对每一个有理素数 $p\nmid N$，令 T_p 为相应的 Hecke 算子，即

$$(T_pf)(\tau)=pf(p\tau)+\sum_{b=0}^{p-1}f\left(\frac{\tau+b}{p}\right);$$

再令W为算子：

$$(Wf)(\tau)=f\left(\frac{-1}{N\tau}\right).$$

则有

$$T_pf=c_pf,\ wf=Wf,\ w=\pm 1.$$

这里的w与函数方程中的w是相同的。

(3) 设ω是 $E/\mathbf{Q}$ 的不变微分。则存在一个定义在$\mathbf{Q}$上的态射ϕ: $X_0(N)\longrightarrow E$，使得$\phi^*(\omega)$是 $X_0(N)$ 上由 $f(\tau)d\tau$ 所表示的微分形式的一个常数倍。这里 $X_0(N)$是由同余子群 $\Gamma_0(N)$ 决定的模曲线，即 $X_0(N)/\mathbb{Q}$ 是一条光滑的射影曲线，并且存在一个复解析同构

$$j_{N,0}:\ \mathbb{H}^*/\Gamma_0(N)\longrightarrow X_0(N)(\mathbf{C}),$$

使得：

设 $\tau\in\mathbb{H}/\Gamma_0(N)$，$\mathbb{K}=\mathbf{Q}(j_{N,0}(\tau))$。则在 $j_{N,0}$ 下，τ 对应于对(pair)$\langle E,\ C\rangle$的一个等价类，其中E为一条椭圆曲线，$C\subset E$ 是一个N阶的循环子群。这个等价类中含有一个 E, C 均在 $\mathbb{K}$ 上定义

的对(pair)(即E是定义在$\mathbb{K}$上的椭圆曲线，而$C\subset E(\overline{\mathbb{K}})$在Galois群$G(\overline{\mathbb{K}}/\mathbb{K})$下映为自己)。

T-W 猜想已对于具有复乘的椭圆曲线证明是成立的，也在许多其他情况下被证明了，参考 LNM 476(参考文献的[101])。

2.3 S-T 群与 BSD 猜想

本小节中，恒设$\mathbb{K}$为数域。

定义 2.6 设$E/\mathbb{K}$为一条椭圆曲线。$E/\mathbb{K}$的一个齐性空间是一条光滑曲线$C/\mathbb{K}$，以及E在C上起一个定义在$\mathbb{K}$上的单可递代数群的作用。也即$E/\mathbb{K}$的一个齐性空间实际上是由一对$(C, +)$组成的，其中$C/\mathbb{K}$为一条光滑曲线，且

$$+: C\times E\to C$$

是定义在$\mathbb{K}$上的一个态射，并且具有如下性质：

(1) $p+O=p$, $\forall p\in C$, 这里O是E的恒等元；

(2) $(p+P)+Q=p+(P\oplus Q)$, $\forall p\in C$, P, $Q\in E$;

(3) $\forall p$, $q\in C$, 存在唯一的$P\in E$, 使$p+P=q$。

定义 2.7 设$E/\mathbb{K}$为一条椭圆曲线，$C/\mathbb{K}$与$C'/\mathbb{K}$为$E/\mathbb{K}$的两个齐性空间。$C/\mathbb{K}$与$C'/\mathbb{K}$称为等价，如果存在一个定义在$\mathbb{K}$上的由C到C'的同构映射θ，且θ满足

$$\theta(p+P)=\theta(p)+P,\ \forall p\in C,\ P\in E.$$

定理 2.4 设$E/\mathbb{K}$为一条椭圆曲线。$E/\mathbb{K}$的齐性空间等价类全体，构成了一个群，称为 Weil-Chatelet 群，记为$WC(E/\mathbb{K})$，它同构于$H^1(G(\overline{\mathbb{K}}/\mathbb{K}), E)$(其中$G(\overline{\mathbb{K}}/\mathbb{K})$是 Galois 群 $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$)，所用的同构映射如下：设$C/\mathbb{K}$为$E/\mathbb{K}$的一个齐性空间，任意选定$p_0\in C$，则$C/\mathbb{K}$的等价类

$$\{C/\mathbb{K}\}\longrightarrow\{\sigma\to p_0^\sigma-p_0\}\in H^1(G(\overline{\mathbb{K}}/\mathbb{K}), E).$$

$WC(E/\mathbb{K})$的恒等元是所谓的显然类，即该类中含有由E及作用于E的平移所组成的齐性空间。一个齐性空间$C/\mathbb{K}$属于显然类的充要条件是$C(\mathbb{K})$非空。

记$M_\mathbb{K}$为$\mathbb{K}$的所有彼此不等价的赋值组成的集合。对每一

个$\nu\in M_{\mathbb{K}}$，也可对$E/\mathbb{K}$定义群$WC(E/\mathbb{K}_\nu)$。由此可得

定义 2.8 设$E/\mathbb{K}$为一条椭圆曲线。定义$E/\mathbb{K}$的Shafarevich-Tate群为$WC(E/\mathbb{K})$的一个如下的子群：

$$Ш(E/\mathbb{K})=\mathrm{Ker}\{WC(E/\mathbb{K})\longrightarrow\prod_{\nu\in M_{\mathbb{K}}}WC(E/\mathbb{K}_\nu)\},$$

即可以想象S-T群$Ш(E/\mathbb{K})$为由$E/\mathbb{K}$的处处均为局部显然的齐性空间，即对每一个$\nu\in M_{\mathbb{K}}$，均有一个$\mathbb{K}_\nu$-点的齐性空间等价类组成的群。

猜想 5.D 对任意一个数域$\mathbb{K}$，和任意一条椭圆曲线$E/\mathbb{K}$，S-T群$Ш(E/\mathbb{K})$是一个有限群，且其阶为一个完全平方的正整数。

K. Rubin首先在1986年证明猜想5.D对一批椭圆曲线是成立的。

设$\mathbb{Q}$为有理数域，$\mathbb{Q}_p$为p-adic数域，$E/\mathbb{Q}$为一条椭圆曲线，并设$E/\mathbb{Q}$为由极小Weierstrass方程

$$E:\ y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \qquad (5.52)$$

给出。方程(5.52)称为极小，如果它满足

(1) $a_i\in\mathbb{Z}$, $i=1, 2, 3, 4, 6$;

(2) 对每一个有理素数p，令E的p-adic极小Weierstrass方程的判别式为Δ_p(参考(5.48))。那么有

$$\Delta=\prod_p p^{\mathrm{ord}_p(\Delta_p)},$$

这里p跑过所有有理素数p，Δ是(5.52)的判别式。

相应于方程(5.52)，$\omega=\dfrac{dy}{2y+a_1x+a_3}$称为$E/\mathbb{Q}$的Néron不变微分，$\Omega=\int_{E(\mathbb{R})}|\omega|$是$E$的实周期或其两倍，这视$E(\mathbb{R})$连通与否而定。

$E/\mathbb{Q}$的S-T群为$Ш(E/\mathbb{Q})$。

对$P=(x_0, x_1, \cdots, x_m)\in\mathbb{P}^m(\mathbb{Q})$，$P$的高定义为

$$H(P)=\prod_{\nu\in M_{\mathbb{Q}}}\max\{|x_o|_\nu, \cdots, |x_m|_\nu\},$$

设$f\in\mathbb{Q}(E)$为任一个非常数的偶函数，且f为实值函数。即应有

$f(-P)=f(P)\in P^1(\mathbb{R})$, $\forall P\in E$. 对 $P\in E$, 令

$$h_f(P)=\log H(f(P)).$$

引理 2.6(Tate) 对每一个 $P\in E(\mathbb{C})$, 极限

$$\frac{1}{\deg f}\lim_{N\to\infty}4^{-N}h_f([2^N]P)$$

存在, 且与 f 的选取无关。

引理中的极限, 称为P 的Néron-Tate 高, 因此定义了 $E/\mathbb{Q}$ 的 Néron-Tate 高函数, 记为 $\hat{h}$。

设 $P_1, \cdots, P_r\in E(\mathbb{Q})$生成了 $E(\mathbb{Q})/E_{tor}(\mathbb{Q})$, 则称

$$R(E/\mathbb{Q})=\det(<P_i, P_j>)_{1<i,j<r}$$

为 $E(\mathbb{Q})/E_{tor}(\mathbb{Q})$ 的正则子(Regulator), 其中

$$<P_i, P_j>=\frac{1}{2}(\hat{h}(P_i+P_j)-\hat{h}(P_i)-\hat{h}(P_j)).$$

$R(E/\mathbb{Q})$ 也称为 $E/\mathbb{Q}$ 的正则子。

对每一个有理素数 p, 令 $E_0(\mathbb{Q}_p)$ 为 $E(\mathbb{Q}_p)$ 在 p-约化后是非奇异点的原象组成的集合, 并记 $c_p=|E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)|$, 那么 $c_p=1$, 如E 在 p 处有好约化; $c_p=-\mathrm{ord}_p(j)\geqslant 1$, 如$E$ 在 p 处有一个 Split 乘法约化, j 是E 的 j-不变量; $1\leqslant c_p\leqslant 4$, 其他情况。

现在我们可以来叙述椭圆曲线 $E/\mathbb{Q}$ 的 BSD 猜想了。

猜想 5.E(Birch-Swinnerton-Dyer) 设 $E/\mathbb{Q}$ 为椭圆曲线, 其余记号如上, 则有:

(1) $E/\mathbb{Q}$ 的 L-函数 $l_E(s)$ 在 $s=1$ 处有一个阶为 $r(=E(\mathbb{Q})$ 的秩)的零点;

(2) 设 $r=\mathrm{rank}\ E(\mathbb{Q})$, 则有

$$\lim_{r\to 1}\frac{L_E(s)}{(s-1)^r}=\Omega|Ш(E/\mathbb{Q})|R(E/\mathbb{Q})|E_{tor}(\mathbb{Q})|^{-2}\prod_p c_p,$$

这里 p 跑过所有的有理素数。

BSD 猜想已被证明对无穷多条椭圆曲线 $E/\mathbb{Q}$ 是成立的。

2.4 一条具体的椭圆曲线的讨论

我们现在讨论 $\mathbb{Q}$ 上椭圆曲线(参见文献[7])

$$E:\ y^2=4x^3-28x+25 \tag{5.53}$$

E 的导子 $N=5077$，这是一个素数。E 是 $\mathbb{Q}$ 上的秩为 3 的椭圆曲线，且是在这种曲线中导子为最小可能的。E 的极小 Weierstrass 方程为（系由 (5.53) 中作变换 $x\mapsto x$, $y\mapsto 2y+1$ 得出）

$$E:\ y^2+y=x^3-7x+6. \tag{5.54}$$

方程(5.54)的判别式 $\Delta=5077=N$。

对由(5.53)或(5.54)所定义的椭圆曲线 E，可取上一小节的偶函数 $f(P)=x(P)$（即 P 的第一个坐标）。于是对 $P\in E(\mathbb{Q})$，有：

$$h(P)=h_f(P)=\log\max(|a|,\ b),$$

$$x(P)=\frac{a}{b},\ b>0,\ a,\ b\in\mathbb{Z},\ g.c.d.(a,\ b)=1. \tag{5.55}$$

由此可得 $E(\mathbb{Q})$ 的 Néron-Tate 高的公式：

$$\hat{h}(P)=\log b+F(x(P)), \tag{5.56}$$

这里 b 是 $x(P)$ 的分母，如(5.55)所示；而 $F(x)$ 为一个如下定义的实值函数：

$$F(x)=\log|x|+\sum_{n=0}^{\infty}4^{-n-1}\log z_n, \tag{5.57}$$

其中

$$z_n=1+14x_n^{-2}-50x_n^{-3}+49x_n^{-4},\ x_0=x,$$

$$x_{n+1}=\frac{x_n^4+14x_n^2-50x_n+49}{4x_n^3-28x_n+25},$$

为了对一切 x 都更方便一些，我们改写(5.57)为

$$F(x)=\frac{1}{4}\log(x^4+14x^2-50x+49)+\sum_{n=1}^{\infty}4^{-n-1}\log z_n, \tag{5.58}$$

事实上，有 $x_n=x(2^nP)$，从而，当 $n\geqslant 1$ 时，有 $x_n\geqslant e_3=1.946\cdots$。这里 $e_1<e_2<e_3$ 表示三次多项式 $4x^3-28x+25$ 的三个根。于是

$$1\leqslant z_n\leqslant 1.328\cdots,\ 0\leqslant\log z_n\leqslant 0.284\cdots,$$

若 $n\geqslant 1$。即级数(5.57)或(5.58)是收敛很快的。我们有

$$0 \leqslant F(x) - \log|x| \leqslant 0.0947\cdots, \text{ 如 } x \geqslant e_3.$$

从而不难证明

$$0 \leqslant F(x) - \log\max(|x|, 1) \leqslant 1.205\cdots,$$

由此及(5.55)与(5.56)有

$$h(P) \leqslant \hat{h}(P) \leqslant h(P) + 1.205\cdots \tag{5.59}$$

用(5.59)不难证明，$E(\mathbb{Q})$中满足 $\hat{h}(P) < 1$ 的无限阶元 P 有且仅有三个：

$P_0 = (0, 2)$，$P_1 = (1, 0)$，$P_2 = (2, 0)$。(用到(5.54))

对每一个有理素数 $p \neq 5077$，命

$$N_p = 1 + |\{x, y \in \mathbb{Z} \mid y^2 + y = x^3 - 7x + 6 (\mathrm{mod}\ p)\}|. \tag{5.60}$$

容易算出 $N_3 = 7$，$N_5 = 10$。由 $|E_{tor}(\mathbb{Q})|$除尽 N_3，N_5，即知应有 $|E_{tor}(\mathbb{Q})| = 1$。因此可以证明 P_0，P_1，P_2 是 $E(\mathbb{Q})$的生成元，即有

$$E(\mathbb{Q}) = \mathbb{Z}P_0 + \mathbb{Z}P_1 + \mathbb{Z}P_2 \tag{5.61}$$

于是正则子

$$\begin{aligned} R(E/\mathbb{Q}) &= \det(\langle P_i, P_j \rangle)_{0 < i,j < 2} \\ &= \det\begin{pmatrix} 0.9909\cdots & -0.2365\cdots & -0.2764\cdots \\ -0.2365\cdots & 0.6682\cdots & 0.0333\cdots \\ -0.2764\cdots & 0.0333\cdots & 0.7670\cdots \end{pmatrix} \\ &= 0.4171435587\cdots \end{aligned} \tag{5.62}$$

E 的 Néron 不变微分 $\omega = \dfrac{dy}{2y+1}$，从而

$$\Omega = \int_{E(\mathbb{R})} |\omega| = 2\int_{E(\mathbb{R})^\circ} |\omega|,$$

这是因为 $E(\mathbb{R})$恰有两个连通分支，$E(\mathbb{R})^\circ$ 为其中任意一支。如把E的方程 (5.53) 改写为$y^2 = 4(x - e_1)(x - e_2)(x - e_3)$，其中 $e_1 < e_2 < e_3$，则有

$$\Omega = 4\int_{e_3}^{\infty} \frac{dx}{y} = \frac{2\pi}{M(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})} = 4.151687\cdots, \tag{5.63}$$

这里对两个正实数x，y，定义

$$M(x, y) = \lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n,$$

其中

$$x_0 = x,\ y_0 = y,\ x_{n+1} = \frac{x_n + y_n}{2},\ y_{n+1} = \sqrt{x_n y_n}.$$

E 的 L-级数在半平面 $\mathrm{Re}\, s > \frac{3}{2}$ 上由下列 Euler 乘积给出

$$L_E(s) = (1 + 5077^{-s})^{-1} \prod_{p \neq 5077} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

$$= \sum_{n=1}^{\infty} a_n n^{-s}, \tag{5.64}$$

这里，当 p 跑过所有理素数，当 $p \neq 5077$ 时，$a_p = p + 1 - N_p$，N_p 由 (5.60) 定义，我们有 $|a_p| \leqslant 2\sqrt{p}$。一般的有 $|a_n| \leqslant \tau(n)\sqrt{n}$，$\tau(n)$ 是 n 的正因子的个数。令

$$\Lambda(s) \stackrel{\text{def}}{=\!=} N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L_E(s) = \int_0^\infty f\left(\frac{iy}{\sqrt{N}}\right) y^{s-1} dy, \tag{5.65}$$

其中 $N = 5077$，和

$$f(\tau) = \sum^{\infty} a_n e^{2\pi i n\tau} (\tau \in \boldsymbol{C},\ \mathrm{Im}\,\tau > 0). \tag{5.66}$$

T-W 猜想断定 $f(\tau)$ 是 $\Gamma_0(N)$ 的权为 2 的一个尖点形式，这个权与这个水平的尖点形式空间 $S_2(N)$ 的维数为 422. 我们可以在 $S_2(N)$ 中进行有限次计算来验证这一点（对每一条具体给定的椭圆曲线 E/Q 都可以用同样方式，经有限步计算来加以验证），但是计算量太大，我们不在此列举了。由此可知 $f(\tau)$ 满足函数方程

$$f\left(\frac{-1}{N\tau}\right) = N\tau^2 f(\tau),$$

从而可以得到 $L_E(s)$ 的解析开拓以及函数方程：

$$\Lambda(s) = \int_1^\infty f\left(\frac{iy}{\sqrt{N}}\right)(y^{s-1} - y^{1-s}) dy = -\Lambda(2-s), \tag{5.67}$$

并且 $\Lambda(s)$ 与 $L_E(s)$ 均为 s 的整函数。

由 (5.67) 即知，$L_E(s)$ 在 $s = 1$ 处的零点的阶是一个奇数，故至少是 1。对任一个正奇数 r，我们有

$$\Lambda^{(r)}(1)=2\int_1^{\infty}f\left(\frac{iy}{\sqrt{N}}\right)(\log y)^r dy$$
$$=2\sum_{n=1}^{\infty}a_n\int_1^{\infty}e^{-2\pi ny/\sqrt{N}}(\log y)^r dy. \tag{5.68}$$

假定 $\Lambda(s)$ 在 $s=1$ 处的零点的阶大于等于 r，则对(5.68)做一次分部积分，即得

$$L_E^{(r)}(1)=\frac{2\pi}{\sqrt{N}}\Lambda^{(r)}(1)=2r!\sum_{n=1}^{\infty}\frac{a_n}{n}G_r\left(\frac{2\pi_n}{\sqrt{N}}\right). \tag{5.69}$$

这里，对 $x>0$，有

$$G_r(x)=\frac{1}{(r-1)!}\int_1^{\infty}e^{-xy}(\log y)^{r-1}\frac{dy}{y}\ (r\geqslant 1) \tag{5.70}$$

可以证明(γ 为 Euler 常数)

$$G_1(x)=\log\frac{1}{x}-\gamma+\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n\cdot n!}x^n,$$

这可用于 x 较小时(例如 $x<3$)的计算，对较大的 $x(x>2)$ 可用下列连分数展开式

$$G_1(x)=\cfrac{e^{-x}}{x+\cfrac{1}{1+\cfrac{1}{x+\cfrac{2}{1+\cfrac{2}{x+\cfrac{3}{1+\cdots}}}}}}$$

还可证明

$$G_3(x)=\frac{1}{6}\left(\log\frac{1}{x}-\gamma\right)^3+\frac{\pi^2}{12}\left(\log\frac{1}{x}-\gamma\right)$$
$$-\frac{\zeta(3)}{3}+\sum_{n=1}^{\infty}\frac{(-1)^{n-1}x^n}{n^3\cdot n!}, \tag{5.71}$$

等等。这样经过计算可以证明

$$|L'_E(1)|\leqslant 10^{-13}. \tag{5.72}$$

由 B.Gross-D.Zagier[24]、J.-L.Waldspurger[106] (或[105]) 以及 B.Mazur-H.P.F.Swinnerton-Dyer[73]，可以证明，存在 $P\in E(Q)$，使

$$L'_E(1)=\alpha\Omega\hat{h}(P), \tag{5.73}$$

这里 α 是一个非零的有理数，$\alpha^{-1}<0.6\times10^{13}\Omega$。

这里的具体过程如下：首先由 Waldspurger[106] (或[105]) 知，可取负的基本判别式 D 及 χ_D，使 $L_E(s)$ 的 χ_D-twist

$$L_E(s, \chi_D)=\sum_{n=1}^{\infty}a_n\chi_D(n)n^{-s}$$

为 E 的 D-twist E_D

$$E_D:\ Dy^2=4x^3-28x+25$$

的 L-级数。E_D/Q 仍是一条椭圆曲线，并且 $L_E(1, \chi_D)\neq0$。

再由 Mazur-Swinnerton-Dyer[73] 可知

$$L_E(1, \chi_D)=\beta\Omega_{E_D},$$

这里 Ω_{E_D} 为 E_D 的周期，β 是一个正的有理数，其分子分母的上界只依赖于 D，且可由所谓的 Modular 符号计算之。

最后由 Gross-Zagier[24] 可知，存在 $P\in E(Q)$ 使

$$L_E(1, \chi_D)L_E'(1)=\Omega\Omega_{E_D}\frac{2\hat{h}(P)}{w_K^2},$$

其中 w_K 为 $K=Q(\sqrt{D})$ 的单位根群的阶，由此即得所需。注意可取 $D=-4$。

这样，当 $L_E'(1)\neq0$ 时，由 (5.73) 可知 $0<\hat{h}(P)<0.6$。我们已知 Nérou-Tate 高 <1 的无限阶元只有 P_0，P_1，P_2。因此 $P=P_0, P_1$ 或 P_2 (注意 $\hat{h}(P)=0$ 当且仅当 P 是有限阶的，在我们这里的情况下，即为 $P=O$)。但可算出

$$\hat{h}(P_i)>0.65(i=0, 1, 2),$$

得出矛盾。这就证明了

$$L_E'(1)=0. \tag{5.74}$$

又可用 (5.71) 算出

$$\lim_{s\to1}\frac{L_E(s)}{(s-1)^3}=2\sum_{n=1}^{\infty}\frac{a_n}{n}G_3\left(\frac{2\pi n}{\sqrt{5077}}\right)\approx1.7318499\cdots \tag{5.75}$$

所以由 (5.74) 与 (5.75) 证明了 $L_E(s)$ 在 $s=1$ 处有一个 3 阶零点。

令 $\lambda(n)$ 为 Liouville 函数，即

$$\lambda(n) = \prod_{p^m \| n} (-1)^m.$$

置

$$\tilde{L}(s) = L_E\left(\frac{s}{2}\right) L_E\left(\frac{s}{2}, \lambda\right) \prod_{p \neq 5077} (1 - p^{1-s})^{-1},$$

其中

$$L_E(s, \lambda) = \sum_{n=1}^{\infty} a_n \lambda(n) n^{-s}.$$

可以证明(见 G.Shimura[91])

$$\tilde{L}(s) = \prod_{p \neq 5077} (1 + p^{1-s})^{-1} \sum_{n=1}^{\infty} \frac{a_n^2}{n^s}, \ \mathrm{Re}(s) > 2. \tag{5.76}$$

并且函数($N = 5077$)

$$\tilde{\Lambda}(s) \overset{\text{def}}{=\!=} N^s (2\pi)^{-s} \Gamma(s) \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \tilde{L}(s) \tag{5.77}$$

可解析开拓为整个 s 平面上的整函数，同时满足函数方程

$$\tilde{\Lambda}(3 - s) = \tilde{\Lambda}(s), \tag{5.78}$$

还可有

$$\tilde{\Lambda}(2) = N \iint_{D_0(N)} |f(\tau)|^2 |d\tau \Lambda d\bar{\tau}| > 0, \tag{5.79}$$

这里 $D_0(N)$是上半平面在 $\Gamma_0(N)$ 下的基域（以上还可参考 A.P.Ogg[85]）。

§ 3 Goldfeld-Gross-Zagier 定理及其证明

在本节中，我们用 § 2.4 的结论来给出 GGZ 定理的证明。这个证明是 J.Oésterlé[84] 给出的，它改进了 D.Goldfeld[22] 的原始证明。

设$-d$ 为一个给定的负的基本判别式，$\mathbb{K} = \mathbb{Q}(\sqrt{-d})$是一个虚二次域，以 $h = h(-d) = h_{\mathbb{K}}$ 记 $\mathbb{K}$ 的类数，我们有下面的定理。

定理 3.1 (Goldfeld-Gross-Zagier-Oésterlé)

在上述记号下，我们有

$$55h(-d) \geqslant \theta(d) \log d,$$

这里

$$\theta(d)=\prod_{p\in P(d)}\left(1-\frac{[2\sqrt{p}]}{p+1}\right),$$

其中 $P(d)$ 表示 d 的所有素因子中除去最大素因子之后所得的集合。

推论

(1) 设 $h(-d)$ 奇，则 $55h(-d)\geqslant\log d$;

(2) 设 $h(-d)\equiv 2\pmod 4$，则 $220h(-d)\geqslant\log d$;

(3) 设 $h(-d)\equiv 4\pmod 8$，则 $660h(-d)\geqslant\log d$;

(4) 设 $h(-d)\leqslant 5$，则 d 已尽数列举于 $p.337$ 的表中。

证明 (1)，(2)，(3)由定理 3.1 立即可得。于是可知 $h(-d)\leqslant 5$ 时，必有 $d\leqslant e^{2640}$。这样(4)由引理 1.1 以及以下引理得出。

引理 3.1 引理 1.1 中所提及的可能的例外域

$$K=Q(\sqrt{-d})$$

的判别式 $-d<0$，满足 $d>e^{3000}$。

这一引理可仿照引理 1.2 的证明证出。

附注 Gauss 最初所计算的类数表，列有 $h(-d)\leqslant 5$ 的，所以我们终于可以最后说：Gauss 的表是完全的！

3.1 一些引理

在给出上述的 GGZO 定理的证明之前，我们先来证明一些引理。设 $-d$, K, h 如上，令 $\chi(*)=\left(\frac{-d}{*}\right)$ 为 Kronecker 符号。K 的 Dedekind ζ-函数 $\zeta_K(s)=\zeta(s)L(s,\chi)$。在 K 的理想类群 $\mathscr{C}_K$ 与判别式为 $-d$ 的正定的有理整系数二元二次原型类群 $\mathscr{C}(-d)$ 之间，我们已建立了下列的一一对应。

对每一个理想类 $\mathscr{C}\in\mathscr{C}_K$，取理想 $\mathfrak{A}\in\mathscr{C}$，令 $\{\omega_1,\omega_2\}$ 为 $\mathfrak{A}$ 的一组有向 $\mathbb{Z}$-基(即要求 $\omega_1\sigma(\omega_2)-\omega_2\sigma(\omega_1)=N(\mathfrak{A})\sqrt{-d}$)，则二元二次型 $q(x,y)=\dfrac{N(x\omega_1+y\omega_2)}{N(\mathfrak{A})}$ 是一个正定的有理整系数二元二次原型。在此对应下，$\mathscr{C}_K$ 的理想类与 $\mathscr{C}(-d)$ 的相似类一一对

应。

在$\mathscr{C}(-d)$的每一类中，都有一个唯一的代表元，它称之为约化型，这个型 $q(x, y)=ax^2+bxy+cy^2$，满足下列条件：

(1) $b^2-4ac=-d$, $g.c.d.(a, b, c)=1$;

(2) $-a<b\leqslant a<c$，或$0\leqslant b\leqslant a=c$。

由此可知，对约化型，我们有

$$1\leqslant a\leqslant\sqrt{\frac{d}{3}},\ \sqrt{\frac{d}{2}}\leqslant c\leqslant\frac{d}{3a},$$

且当 $d\neq4$ 时，有 $c>\frac{\sqrt{d}}{2}$。

对这个约化的二次型 q，以 $N_q(t)$ 表示满足 $q(m, n)\leqslant t$ 的整数组 $(m, n)\in\boldsymbol{Z}\times\mathbb{N}$ 的组数。易见 $t<c$ 时，有 $N_q(t)=0$；特别的，当 $t<\frac{\sqrt{d}}{2}$ 时，$N_q(t)=0$。当 $t\to\infty$ 时，易见 $N_q(t)\sim\frac{\pi}{\sqrt{d}}t$。不难证明

$$\int_0^A N_q(t)dt\leqslant\int_{\frac{\sqrt{d}}{2}}^A\frac{\pi t}{\sqrt{d}}dt,\ \forall\,\frac{\sqrt{d}}{2}\leqslant A. \tag{5.80}$$

以下以 $\mathfrak{B}$ 表示所有判别式为$-d$ 的且为约化的正定有理整系数二元二次原型的全体，于是$|\mathfrak{B}|=h$。对 $q\in\mathfrak{B}$，以 $a(q)$ 记 q 的第一个系数。

对每一个类 $\mathscr{C}\in\mathscr{C}_{\boldsymbol{K}}$，我们取相应的 $q\in\mathfrak{B}$，使 q 对应于 $\mathscr{C}$，则类 $\mathscr{C}$ 的 ζ-函数

$$\zeta(s|\mathscr{C})\overset{\text{def}}{=\!=}\sum_{\mathfrak{A}\in\mathscr{C}}(N\mathfrak{A})^{-s}=\frac{1}{w_{\boldsymbol{K}}}\sum_{(m,n)\in\boldsymbol{Z}^2}{}' q(m, n)^{-s}, \tag{5.81}$$

这里求和号上的“′”表示 $(m, n)\neq(0, 0)$；$w_{\boldsymbol{K}}$ 是 $\boldsymbol{K}$ 的单位群的阶。从而可知当 $d>4$ 时，有

$$\begin{aligned}\zeta_{\boldsymbol{K}}(s)&=\sum_{\mathscr{C}\in\mathscr{C}_{\boldsymbol{K}}}\zeta(s|\mathscr{C})\\&=\sum_{q\in\mathfrak{B}}\Big(a(q)^{-s}\zeta(2s)+\sum_{(m,n)\in\boldsymbol{Z}\times\boldsymbol{N}}q(m, n)^{-s}\Big),\end{aligned} \tag{5.82}$$

于是得到，如$d>4$，则有(p表有理素数)

$$\frac{\zeta_{\mathbb{K}}(s)}{\zeta(2s)}=\prod_{p}\frac{1+p^{-s}}{1-\chi(p)p^{-s}}$$
$$=\sum_{q\in\mathfrak{W}}\Big(a(q)^{-s}+\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{N}\\ g.c.d.(m,n)=1}}q(m,n)^{-s}\Big)。\qquad(5.83)$$

引理3.2 (a)设有理素数p在$\mathbb{K}$中分裂，即$\chi(p)=1$时，必有 $p^h\geqslant\frac{d}{4}$。

(b) 设 $\frac{\zeta_{\mathbb{K}}(s)}{\zeta(2s)}=\sum_{n=1}^{\infty}\nu_n n^{-s}(\mathrm{Re}\ s>1)$，其中$\nu_n$为非负整数，则当$d>4$时有

$$\sum_{1<n<\frac{\sqrt{d}}{2}}\nu_n\leqslant h。\qquad(5.84)$$

证明 (a)由假设可知，在$\mathbb{K}$中存在一个范为p的素理想$\mathfrak{P}$，且$p=\mathfrak{P}\overline{\mathfrak{P}}$，$\overline{\mathfrak{P}}$是另一个素理想，$\overline{\mathfrak{P}}\neq\mathfrak{P}$。$\mathfrak{P}$的$h$次幂是一个主理想。即知存在$a\in\mathbb{Z}$及$b\in\mathbb{N}$，使$\mathfrak{P}^h=\frac{a+ib\sqrt{d}}{2}O_{\mathbb{K}}$ ($O_{\mathbb{K}}$是$\mathbb{K}$的整数环)。这样取范之后，即得$p^h=\frac{a^2+b^2d}{4}\geqslant\frac{d}{4}$。

(b) 由(5.83)，当$d>4$时，对$q\in\mathfrak{W}$可知q的最后一个系数大于$\frac{\sqrt{d}}{2}$，从而$N_q\left(\frac{\sqrt{d}}{2}\right)=0$，即可得到所需的结论(5.84)。

对两个Dirichlet级数$A=\sum_{n=1}^{\infty}a_n n^{-s}$与$B=\sum_{n=1}^{\infty}b_n n^{-s}$，引进下列记号，如果$|a_n|\leqslant b_n$对一切$n\geqslant1$均成立，则记为$A\ll B$，称为$A$弱于$B$或$B$强于$A$。

引理3.3 令$U=\left(\frac{\sqrt{d}}{2}\right)^{\frac{1}{m}}$，这里当$h=4$时，$m=\frac{3}{2}$；而当$h\neq4$时，$m$是使$m^2+m\geqslant\frac{h}{2}$成立的最小正整数，那么在小于等于$U$的有理素数中，至多有一个是在$\mathbb{K}$中为分裂的；如果$p$是一个这样的素数，则必有$p\geqslant\left(\frac{d}{4}\right)^{\frac{1}{h}}$。最后可知$d$的最大素因子大于

U。

证明 设 p, p_1 为两个不同的有理素数，它们均在 $\mathbb{K}$ 中分裂，且 p, $p_1 \leqslant U$。则由 $\frac{\zeta_{\mathbb{K}}(s)}{\zeta(2s)}$ 的 Euler 乘积可知有

$$\frac{1+p^{-s}}{1-p^{-s}} \cdot \frac{1+p_1^{-s}}{1-p_1^{-s}} \ll \frac{\zeta_{\mathbb{K}}(s)}{\zeta(2s)}, \tag{5.85}$$

(5.85)的左边是

$$\left(1+2\sum_{l=1}^{\infty} p^{-ls}\right)\left(1+2\sum_{l_1=1}^{\infty} p_1^{-l_1 s}\right) \xlongequal{\text{def}} \sum_{n=1}^{\infty} \frac{\lambda_n}{n^s}. \tag{5.86}$$

现在我们考虑满足条件 $l+l_1 \leqslant m' = [m]$ 的所有的非负整数组(l, l_1)。对每一个这样的组，有

$$p^l p_1^{l_1} \leqslant U^{l+l_1} \leqslant \frac{\sqrt{d}}{2}.$$

故由(5.86)、(5.85)和(5.84)即有

$$h \geqslant \sum_{1<n<\frac{\sqrt{d}}{2}} \nu_n \geqslant \sum_{1<n<\frac{\sqrt{d}}{2}} \lambda_n \geqslant 1+2m'+2m' + 4\frac{m'(m'-1)}{2} = 2m'^2+2m'+1 \geqslant h+1,$$

这是一个矛盾，于是至多只可能有一个小于等于U的有理素数 p 在 $\mathbb{K}$ 中分裂，至于可能的这个素数 $p \geqslant \left(\frac{d}{4}\right)^{\frac{1}{h}}$ 是引理 3.2 的结论。最后一个结论可如下证明之。

设 T 为 d 的不同素因子的个数，则由 genus 理论可知 2^{T-1} 除尽 h。由此可知 $T \leqslant 2m$。这是因为当 $h=4$ 时，$T \leqslant 3$，但 $m=\frac{3}{2}$，立见 $T \leqslant 2m$；而当 $h \neq 4$ 时，由 $m^2+m \geqslant 2^{T-2}$ 且m 为正整数，即可有 $T \leqslant 2m$(否则 $T \geqslant 2m+1$，于是$(2m+1)^2 \geqslant 2^{2m+1}+1$，这只有 $m=1$ 时才可能，从而必有 $h=1, 2, 3$，所以 $T \leqslant 2 = 2m$ 得出矛盾)。对给定的负基本判别式$-d$，d 或 $\frac{d}{4}$ 是一个无平方因子的正整数，于是 d 的最大素因子 $p \geqslant \left(\frac{d}{4}\right)^{\frac{1}{T}} \geqslant U$，由此不难证明$p > U$。引理证毕。

引理 3.4 设有理整数 $m\geqslant 2$, a 与 σ 均为实数, 且 $\sigma>a$. 则

$$I(x)=\int_{\sigma-i\infty}^{\sigma+i\infty}x^{-s}(s-a)^{-m}\frac{ds}{2\pi i}(\mathrm{Re}\,s=\sigma,\ x>0)$$

是 $(0,\ +\infty)$ 中的正函数, 且当 $a\geqslant 0$ 时为下降的凸函数。

证明 这是因为对 $x>0$。有

$$I(x)=\begin{cases}x^{-a}\dfrac{|\log x|^{m-1}}{(m-1)!}, & \text{如 } 0<x\leqslant 1;\\ 0, & \text{如 } x\geqslant 1.\end{cases}$$

引理从而成立。

设正整数 $m\geqslant 2$, a 与 σ 为两个实数, 且 $\sigma>a$。再设 μ_1, $\cdots$, μ_r 为 $\mathbb{R}_+^*=(0,\ +\infty)$ 中的正测度, 且它们均使函数 $t\mapsto t^{-\sigma}(t\in\mathbb{R}_+^*)$ 为可积的。令

$$\hat{\mu}_j(s)=\int_{\mathbb{R}_+^*}t^{-s}\mu_j,\ 1\leqslant j\leqslant r,$$

以及

$$J(x)=\int_{\sigma-i\infty}^{\sigma+i\infty}\hat{\mu}_1(s)\cdots\hat{\mu}_r(s)x^{-s}(s-a)^{-m}\frac{ds}{2\pi i}\ (\mathrm{Re}s=\sigma,\ x>0).$$

引理 3.5 上述定义的 $J(x)$ 是 $\mathbb{R}_+^*$ 上的一个正函数, 且当 $a\geqslant 0$ 时, 是一个下降的凸函数。

证明 这是上述引理 3.4 及 Fubini 定理的推论。

例 1 对 $u<\sigma$, 令 $\mu=(e^{-t}t^{-u-1}dt)_{t\mapsto t^{-1}}$, 则

$$\hat{\mu}(s)=\Gamma(s-u).$$

例 2 设 $(a_n)_{n\geqslant 1}$ 为一个正实数序列, 且使 $\sum\limits_{n\geqslant 1}a_nn^{-\sigma}$ 收敛。令

$$\mu=\sum_{n=1}^{\infty}a_n\delta_n,$$

这里 δ_n 是对点 n 的 Dirac 测度。则

$$\hat{\mu}(s)=\sum_{n=1}^{\infty}a_nn^{-s}.$$

引理 3.6 设 $\mu_j'(1\leqslant j\leqslant r)$ 为 $\mathbb{R}_+^*$ 的正测度, 并满足上述与 $\mu_j(1\leqslant j\leqslant r)$ 所满足的同样的条件, 类似于 J 可以定义 J'。再设

$$\int_0^x\mu_j([0,\ t])dt\leqslant\int_0^x\mu_j'([0,\ t])dt,\ x>0,\ 1\leqslant j\leqslant r.$$

则当 $a\geqslant 0$ 时，有 $J(x)\leqslant J'(x)$, $x\in\mathbb{R}_+^*$.

证明 先证 $r=1$ 时的情形，这时有

$$J(x)=\int_{\mathbb{R}_+^*} I(xt)\mu_1,\ J'(x)=\int_{\mathbb{R}_+^*} I(xt)\mu_1'.$$

由引理 3.4 可知函数 $t\longmapsto I(xt)$ $(t\in\mathbb{R}_+^*)$ 是正的下降的凸函数，故由引理的假设即知 $r=1$ 时引理成立。$r\geqslant 2$ 时可用归纳法而得出本引理.

例 3 设 $q\in\mathfrak{Q}$, 即 q 为一个判别式 $=-d$ 的约化的正定的有理整系数二元二次原型，取 μ 为所有 Dirac 测度 $\delta_{q(m,n)}$ $((m,n)\in\mathbb{Z}\times\mathbb{N})$ 的和，而 μ' 为 $\frac{\pi}{2}\delta_{\frac{\sqrt{d}}{2}}$ 与 $\left[\frac{\sqrt{d}}{2},+\infty\right)$ 上的 Lebesque 测度的 $\frac{\pi}{\sqrt{d}}$ 倍的和。由(5.80)即有

$$\int_0^x\mu([0,t])dt\leqslant\int_0^x\mu'([0,t])dt\quad(x>0)$$

成立。对 $\operatorname{Re}s=\sigma>1$, 有

$$\hat{\mu}(s)=\sum_{(m,n)\in\mathbb{Z}\times\mathbb{N}}q(m,n)^{-s},\quad \hat{\mu}'(s)=\frac{\pi}{2}\frac{s}{s-1}\left(\frac{\sqrt{d}}{2}\right)^{-s}.$$

例 4 令 $\nu=\sum_{n=1}^{\infty}\delta_n$, 其中 δ_n 为 Dirac 测度；ν' 是 δ_1(Dirac 测度)与 $[1,+\infty)$ 的 Lebesque 测度的和，再令 ν 与 ν' 在变换 $t\mapsto t^2$ 下的象分别是 μ 与 μ'。由 $\nu([0,t])\leqslant\nu'([0,t])$ $(t>0)$ 即得

$$\mu([0,t])\leqslant\mu'([0,t])\ (t>0).$$

当 $\operatorname{Re}s=\sigma>1$ 时，

$$\hat{\mu}(s)=\zeta(2s),\ \hat{\mu}'(s)=\frac{s}{s-\frac{1}{2}}.$$

3.2 GGZO 定理的证明(一)

命 E 为 §2.4 中给出的椭圆曲线，

$$f(\tau)=\sum_{n=1}^{\infty}a_ne^{2\pi in\tau}$$

为那里的尖点形式。令

$$f_\chi(\tau)=\sum_{n=1}^{\infty}a_n\chi(n)e^{2\pi i n\tau}\quad(\tau\in H,\ H\text{ 是上半平面}),\tag{5.87}$$

这里 $\chi(*)=\left(\frac{-d}{*}\right)$为上小节中给出的 Kronecker 符号，$f_\chi$ 称为 f 的 χ-twist. 由参考文献[90]和[105]可知,f_χ 仍是一个权为 2 的尖点形式，它的水平 (level) N_χ 可如下决定之：首先已知 $N=5077$ 为一个素数，而

$$N_\chi=\begin{cases}d^2N, & \text{如 } N\nmid d;\\ d^2, & \text{如 } N\mid d.\end{cases}\tag{5.88}$$

再命

$$L_E(s,\chi)=\sum^{\infty}\frac{a_n\chi(n)}{n^s},\ \mathrm{Re}s>\frac{3}{2},\tag{5.89}$$

则可知,$L_E(s,\chi)$可以解析开拓到整个 s 平面成为一个整函数，并且满足函数方程

$$\Lambda_\chi(s)\overset{\text{def}}{=\!=}N_\chi^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L_E(s,\chi)=w_\chi\Lambda_\chi(2-s),\tag{5.90}$$

同时 $\Lambda_\chi(s)$ 也是 s 的整函数，方程(5.90)中的 $w_\chi=\pm1$，还有

$$w_\chi=\begin{cases}\chi(N), & \text{如 } N\nmid d;\\ -1, & \text{如 } N\mid d.\end{cases}\tag{5.91}$$

如 $N\nmid d$ 时，也有 $\chi(N)=1$ 的话，则由引理 3.2 有

$$N^h\geqslant\frac{d}{4},\ \text{故 } h\log 5077\geqslant\log\frac{d}{4},$$

所以当

$$d>\exp\left\{\frac{55\log 4}{55-\log 5077}\right\}>6$$

时，即有

$$55h>\theta(a)\log d,\tag{5.92}$$

而 $d\leqslant6$ 时，$d=3,4$，(5.92) 仍然成立。这样当 $N\nmid d$ 时，可设 $\chi(N)=-1$。这说明，由 (5.91) 可知，总可以设 $w_\chi=-1$，即 $\Lambda_\chi(s)$满足函数方程

$$\Lambda_\chi(s)=-\Lambda_\chi(2-s).\tag{5.93}$$

特别有 $\Lambda_\chi(1)=0$, 即 $\Lambda_\chi(s)$ 在 $s=1$ 处至少有一阶零点(显然 $\Lambda_\chi(s)$ 在 $s=1$ 处零点的阶是一个奇数)。

命 $M=\frac{\sqrt{NN_\chi}}{4d\pi^2}$, 则有

$$M=\begin{cases}\frac{N}{4\pi^2}, & \text{如 } N\nmid d;\\ \frac{\sqrt{N}}{4\pi^2}, & \text{如 } N\mid d.\end{cases} \tag{5.94}$$

命 $\lambda(n)$ 为 Liouville 函数, $L_E(s,\lambda)$ 如 §2.4. 再命

$$\Psi(s)=L_E(s)L_E(s,\lambda),\quad G(s)=L_E(s,\chi)L_E(s,\lambda)^{-1} \tag{5.95}$$

则有

$$\Psi(s)=(1-N^{-2s})^{-1}\prod_{p\nmid N}(1-\alpha_p^2p^{-2s})^{-1}(1-\bar{\alpha}_p^2p^{-2s})^{-1},\quad \mathrm{Re}s>1, \tag{5.96}$$

这里由 P. Deligne 所证明的 A. Weil 猜想可知 α_p 与 α_p 的复共轭 $\bar{\alpha}_p$ 满足

$$\alpha_p+\bar{\alpha}_p=a_p,\quad |\alpha_p|=\sqrt{p},\ \text{当 } p\nmid N, \tag{5.97}$$

p 表素数。因此, (5.96) 右边的 Euler 乘积在 $\mathrm{Re}s>1$ 时绝对收敛, 从而还可有

$$\Psi(s)\lll\zeta(2s-1)^2, \tag{5.98}$$

即 $\zeta(2s-1)^2$ 强于 $\Psi(s)$。

也不难证明(注意 $N=5077$)

$$G(s)=\frac{1-5077^{-s}}{1+\chi(N)5077^{-s}}\prod_{p\nmid N}\frac{(1+\alpha_pp^{-s})(1+\bar{\alpha}_pp^{-s})}{(1-\alpha_p\chi(p)p^{-s})(1-\bar{\alpha}_p\chi(p)p^{-s})},$$
$$\mathrm{Re}s>\frac{3}{2}, \tag{5.99}$$

右边的 Euler 乘积在 $\mathrm{Re}s>\frac{3}{2}$ 时绝对收敛。由 $|\alpha_p|=\sqrt{p}$ ($p\nmid N$)可得

$$G(s)\lll\left(\frac{\zeta_K\left(s-\frac{1}{2}\right)}{\zeta(2s-1)}\right)^2, \tag{5.100}$$

这可分别对 $\chi(p)=0$, ±1 处理之而得出证明。

由 2.4 小节及本小节的上述关于 $L_E(s,\chi)$ 的定义及其性质的阐述可知，函数

$$F(s)\xlongequal{\text{def}}d^sM^s\Gamma(s)^2L_E(s)L_E(s,\chi)$$
$$=d^sM^s\Gamma(s)^2G(s)\Psi(s)=\Lambda(s)\Lambda_\chi(s)$$

具有下列性质：

(1) $F(s)$是 s 的整函数；

(2) $F(s)$在 $s=1$ 处有一个至少为四阶的零点；

(3) $F(s)$满足函数方程 $F(s)=F(2-s)$。

再由定义(5.95)及 2.4 小节可知，

$$\Psi(s)=L_E(s)L_E(s,\lambda)=\tilde{L}(2s)\prod_{p\nmid N}(1-p^{1-2s})$$
$$=\prod_{p\nmid N}\frac{1-p^{1-2s}}{1+p^{1-2s}}\sum_{n=1}^{\infty}\frac{a_n^2}{n^{2s}},\ \mathrm{Re}s>1,\tag{5.101}$$

右边的级数在 $\mathrm{Re}s>1$ 中，是绝对收敛的（用 $|a_n|\leqslant\tau(n)\sqrt{n}$，$\tau(n)$是 n 的正因子的个数），所以$\Psi(s)$ 在 $\mathrm{Re}s>1$ 中是解析的。由

$$\prod_{p\nmid N}(1-p^{-2s})=\frac{1}{(1-N^{1-2s})\zeta(2s-1)},\ \mathrm{Re}s>1$$

及$\tilde{L}(s)$为整函数(见 § 2.4)，故 $\Psi(s)$是 s 的半纯函数，并有

$$\Psi(s)=\frac{N^{-2s}(2\pi)^{2s}\pi^s\tilde{\Lambda}(2s)}{\Gamma(2s)\Gamma(s)(1-N^{1-2s})\zeta(2s-1)},\ s\in\mathbf{C},\tag{5.102}$$

其中 $\tilde{\Lambda}(s)$是在 § 2.4 中定义的整函数。于是$\Psi(s)$在 $\mathrm{Re}\,s\geqslant1$ 中解析，且 $s=1$ 是 $\Psi(s)$的一个单零点，同时

$$\lim_{s\to1}\frac{\Psi(s)}{s-1}=\frac{8\pi^3}{N(N-1)}\tilde{\Lambda}(2)>0。\tag{5.103}$$

由 G.Shimura[91]，不难得知，对给定的正实数 $\sigma_2>\sigma_1\geqslant1$，有下列估计：

$$M^s\Gamma(s)^2\Psi(s)=O(e^{-\frac{\pi}{2}|t|}),\ s=\sigma+it,\ \sigma_1<\sigma<\sigma_2,\tag{5.104}$$

这里 O 所含的正常数仅与 σ_1, σ_2 有关。

由模形式的一般理论可知，$F(s)$ 也满足类似的估计，即有：

$$F(s)=O(e^{-\frac{\pi}{2}|t|}),\ s=\sigma+it,\ \sigma_1<\sigma<\sigma_2, \qquad (5.105)$$

这里 O 所含正常数仅与 σ_1, σ_2 有关。

命

$$I=\int_{2-i\infty}^{2+i\infty}\frac{F(s)ds}{2\pi id(s-1)^3}. \qquad (5.106)$$

注意分母上的 d 是使 $-d$ 为负基本判别式的正整数。

由 $F(s)$ 的性质可知，(5.106)右边的积分绝对收敛，故 I 有意义，再由 $F(s)$ 的性质可知

$$I=\int_{1-i\infty}^{1+i\infty}\frac{F(s)ds}{2\pi id(s-1)^3}=i\int_{-\infty}^{+\infty}\frac{F(1+it)dt}{2\pi dt^3}$$
$$=i\int_{-\infty}^{+\infty}\frac{F(1-it)}{2\pi dt^3}dt=-i\int_{-\infty}^{+\infty}\frac{F(1+it)}{2\pi dt^3}dt=-I,$$

以上先用 $F(s)$ 的函数方程，再作变换 $t\longmapsto -t$。因此 $I=0$。即有

$$\int_{2-i\infty}^{2+i\infty}\frac{F(s)ds}{2\pi id(s-1)^3}=0. \qquad (5.107)$$

3.3 GGZO 定理的证明(二)

不妨设 $d\geqslant 4$。于是 §3.1 中定义的 $U\geqslant 1$。对 $\mathrm{Re}\,s>\frac{3}{2}$，命

$$G(U,s)=\prod_{p<U}G_p(s), \qquad (5.108)$$

这里 p 表素数，$G_p(s)$ 是 $G(s)$ 的 Euler 乘积中的 p 部分，即

$$G_p(s)=\begin{cases}1, & \text{如 } p=N;\\ \dfrac{(1+\alpha_p p^{-s})(1+\bar{\alpha}_p p^{-s})}{(1-\alpha_p\chi(p)p^{-s})(1-\bar{\alpha}_p\chi(p)p^{-s})}, & \text{如 } p\neq N.\end{cases} \qquad (5.109)$$

再命

$$G_1(U,s)=G(s)-G(U,s)=G(U,s)\Big(\prod_{p>U}G_p(s)-1\Big), \qquad (5.110)$$

$$J(U)=\int_{2-i\infty}^{2+i\infty}\frac{d^s M^s \Gamma(s)^2\Psi(s)G(U,\ s)ds}{2\pi i d(s-1)^3}, \qquad (5.111)$$

$$J_1(U)=\int_{2-i\infty}^{2+i\infty}\frac{d^s M^s \Gamma(s)^2\Psi(s)G_1(U,\ s)ds}{2\pi i d(s-1)^3}. \qquad (5.112)$$

由上小节的(5.101)已知 $I=0$，即知有

$$J(U)=-J_1(U). \qquad (5.113)$$

由于 $\Psi(s)$ 有表达式(5.102)，我们可对 (5.111) 右边的积分改取一个路径

$$\Gamma:\ \{1-it\,|+\infty>t\geqslant\eta'\}\cup\{\sigma-i\eta'\,|1\geqslant\sigma\geqslant1-\eta\}\cup\{1-\eta+it\,|-\eta'\leqslant t\leqslant\eta'\}\cup\{\sigma+i\eta'\,|1-\eta\leqslant\sigma\leqslant1\}\cup\{1+it\,|\eta'\leqslant t<+\infty\},$$

这里实数 η 满足$0<\eta\leqslant\frac{1}{4}$，正实数 η' 适当选取，以使 $\Psi(s)$ 在 Γ 与 $\mathrm{Re}s=2$ 所界的区域内解析。这样，由于 $\Psi(s)$ 在 $s=1$ 处有一个单零点，用(5.100)、(5.104)、(5.108)和(5.111)以及残数定理，可得

$$J(U)=c_1G(U,\ 1)\left(\log d+\frac{G'(U,\ 1)}{G(U,\ 1)}+c_2\right)+J_0(U), \qquad (5.114)$$

这里我们已设

$$M^s\Gamma(s)^2\Psi(s)=c_1(s-1)+c_1c_2(s-1)^2+O(|s-1|^3),\ s\to1 \qquad (5.115)$$

其中

$$c_1=\frac{8M\pi^3}{N(N-1)}\tilde{\Lambda}(2)>0,$$

$$c_2=2\frac{\tilde{\Lambda}'(2)}{\tilde{\Lambda}(2)}+\log(4M\pi^3)-2\gamma-\frac{2N}{N-1}\log N, \qquad (5.116)$$

而 $J_0(U)$ 的定义为

$$J_0(U)=\int_\Gamma\frac{d^s M^s\Gamma(s)^2\Psi(s)G(U,\ s)ds}{2\pi i d(s-1)^3}. \qquad (5.117)$$

$J_0(U)$ 有下列的估计

$$|J_0(U)| \leqslant c_3 \sup_{s \in \Gamma} |G(U, s)|, \tag{5.118}$$

这里

$$c_3 = \int_\Gamma |M^s \Gamma(s)^2 \Psi(s)(s-1)^{-3}| \frac{|ds|}{2\pi} \tag{5.119}$$

是一个与 d 无关的常数。

由(5.112)有

$$J_1(U) = \int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty} d^{s-\frac{1}{2}} M^{s+\frac{1}{2}} \Gamma\left(s+\frac{1}{2}\right)^2 \Psi\left(s+\frac{1}{2}\right)$$

$$G_1\left(U, s+\frac{1}{2}\right)\left(s-\frac{1}{2}\right)^{-3} \frac{ds}{2\pi i}. \tag{5.120}$$

从(5.98)与(5.100)可得

$$\Psi\left(s+\frac{1}{2}\right) \ll \zeta(2s)^2, \quad G\left(s+\frac{1}{2}\right) \ll \left(\frac{\zeta_K(s)}{\zeta(2s)}\right)^2, \tag{5.121}$$

故由 §3.1 的(5.83)、(5.121)、(5.108)和(5.110)即有

$$\Psi\left(s+\frac{1}{2}\right) G_1\left(U, s+\frac{1}{2}\right) \ll \Phi(s), \tag{5.122}$$

这里 $\Phi(s)$ 是一个 Dirichlet 级数，它是在 Dirichlet 级数

$$\left(\sum_{q \in \mathfrak{A}} a(q)^{-s} \zeta(2s) + \sum_{(m,n) \in \mathbb{Z} \times \mathbb{N}} q(m, n)^{-s}\right)^2$$

中去掉满足 $a(q)a(q') < U$ 的形如 $a(q)^{-s} a(q')^{-s} \zeta(2s)^2$ 的 Dirichlet 级数的各项之后而得到的。

用(5.120)、(5.122)，可得

$$|J_1(U)| \leqslant \int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty} d^{s-\frac{1}{2}} M^{s+\frac{1}{2}} \Gamma\left(s+\frac{1}{2}\right)^2 \Phi(s)\left(s-\frac{1}{2}\right)^{-3} \frac{ds}{2\pi i}$$

$$\leqslant \sum_{\substack{q, q' \in \mathfrak{A} \\ a(q)a(q') > U}} \int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty} d^{s-\frac{1}{2}} M^{s+\frac{1}{2}} \Gamma\left(s+\frac{1}{2}\right)^2$$

$$\cdot \frac{\zeta(2s)^2\left(s-\frac{1}{2}\right)^{-3}}{a(q)^s a(q')^s} \frac{ds}{2\pi i}$$

$$+ 2 \sum_{q, q' \in \mathfrak{A}} \int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty} d^{s-\frac{1}{2}} M^{s+\frac{1}{2}} \frac{\zeta(2s)\left(s-\frac{1}{2}\right)^{-3}}{a(q)^s}$$

$$\cdot \sum_{(m,n)\in Z\times N} q'(m,n)^{-s}\frac{ds}{2\pi i}$$

$$+\sum_{q,q'\in \mathfrak{A}}\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty} d^{s-\frac{1}{2}}M^{s+\frac{1}{2}}\Gamma\left(s+\frac{1}{2}\right)^2\sum_{(m,n)\in Z\times N}$$

$$\cdot\, q(m,n)^{-s}\sum_{(m_1,n_1)\in Z\times N} q'(m_1,n_1)^{-s}\frac{\left(s-\frac{1}{2}\right)^{-3}ds}{2\pi i},$$

由此再用引理 3.6 以及 §3.1 的例 1—例 4 的结论，即有

$$|J_1(U)|\leqslant J_1+J_2+J_3, \tag{5.123}$$

其中

$$J_1=h^2\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty} d^{s-\frac{1}{2}}M^{s+\frac{1}{2}}\Gamma\left(s+\frac{1}{2}\right)^2U^{-s}s^2\left(s-\frac{1}{2}\right)^{-5}\frac{ds}{2\pi i}, \tag{5.124}$$

$$J_2=\pi h\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty} 2^s d^{\frac{s-1}{2}}M^{s+\frac{1}{2}}\Gamma\left(s+\frac{1}{2}\right)^2\frac{s}{s-1}$$

$$\cdot\sum_{q\in\mathfrak{A}} a(q)^{-s}\zeta(2s)\frac{\left(s-\frac{1}{2}\right)^{-3}ds}{2\pi i}, \tag{5.125}$$

$$J_3=\frac{\pi^2}{4}\frac{h^2}{\sqrt{d}}\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty} 4^sM^{s+\frac{1}{2}}\Gamma\left(s+\frac{1}{2}\right)^2$$

$$\cdot\left(\frac{s}{s-1}\right)^2\left(s-\frac{1}{2}\right)^{-3}\frac{ds}{2\pi i}, \tag{5.126}$$

由 (5.124) 不难证明

$$J_1=\frac{h^2M}{\sqrt{U}}\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty}\left(\frac{dM}{U}\right)^{s-\frac{1}{2}}\Gamma\left(s+\frac{1}{2}\right)^2s^2\left(s-\frac{1}{2}\right)^{-5}\frac{ds}{2\pi i}$$

$$\leqslant\frac{h^2M}{\sqrt{U}}\left(\frac{1}{4!}\frac{d^4}{ds^4}\left(\Gamma\left(s+\frac{1}{2}\right)^2\left(\frac{dM}{U}\right)^{s-\frac{1}{2}}s^2\right)\right.$$

$$\left.+\frac{1}{3!}\frac{d^2}{ds^2}\left(\Gamma\left(s+\frac{1}{2}\right)^2\left(\frac{dM}{U}\right)^{s-\frac{1}{2}}\right)\right)\Bigg|_{s=\frac{1}{2}}$$

$$=\frac{h^2M}{96\sqrt{U}}P\left(\log\frac{dM}{U}\right), \tag{5.127}$$

这里 $P(x)$ 是 x 的四次多项式：

$$\begin{aligned}P(x) &= x^4 + (16+8\Gamma'(1))x^3 + (64+96\Gamma'(1)+12\Gamma'(1)^2 \\ &\quad +12\Gamma''(1))x^2 + (256\Gamma'(1)+96\Gamma''(1)+96\Gamma'(1)^2 \\ &\quad +8\Gamma^{(3)}(1)+24\Gamma'(1)\Gamma''(1)x+128\Gamma'(1)^2 \\ &\quad +128\Gamma''(1)+96\Gamma'(1)\Gamma''(1)+32\Gamma^{(3)}(1) \\ &\quad +6\Gamma''(1)^2+8\Gamma'(1)\Gamma^{(3)}(1)+2\Gamma^{(4)}(1).\end{aligned}$$

利用 $\Gamma'(x)=\Gamma(x)\psi(x)$，$\psi(1)=-\gamma$，$\psi^{(k)}(1)=(-1)^{k+1}k!\zeta\cdot(k+1)\ (k\geqslant 1)$，可以证明

$$P(x)\leqslant x^4+12x^3+37x^2+27x+108\leqslant(x+3.3)^4,\ \text{如}\ x>0, \tag{5.128}$$

由(5.127)与(5.128)即得

$$J_1\leqslant\frac{M}{96}\frac{h^2}{\sqrt{U}}\left(3.3+\left|\log\frac{dM}{U}\right|\right)^4. \tag{5.129}$$

类似的可由(5.125)得到

$$\begin{aligned}J_2 &= \sum_{q\in\mathfrak{A}}\pi h\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty} a(q)^{-s}2^s d^{\frac{s-1}{2}} M^{s+\frac{1}{2}}\Gamma\left(s+\frac{1}{2}\right)^2 \\ &\quad\cdot\zeta(2s)\frac{s\left(s-\frac{1}{2}\right)^{-3}}{s-1}\frac{ds}{2\pi i} \\ &\leqslant\sum_{q\in\mathfrak{A}}8\pi h\left(a(q)^{-s}2^s d^{\frac{s-1}{2}} M^{s+\frac{1}{2}}\zeta(2s)\Gamma\left(s+\frac{1}{2}\right)^2\right)\Big|_{s=1},\end{aligned}$$

由此即得

$$J_2\leqslant\frac{2\pi^4}{3}M^{\frac{3}{2}}h\sum_{q\in\mathfrak{A}}a(q)^{-1}. \tag{5.130}$$

对任意的正数 ε，如 $0<\varepsilon<1$，则由(5.126)有

$$\begin{aligned}J_3 &= \frac{\pi^2h^2}{4\sqrt{d}}\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty}4^sM^{s+\frac{1}{2}}\Gamma\left(s+\frac{1}{2}\right)^2\frac{s^2}{(s-1)^2}\left(s-\frac{1}{2}\right)^{-3}\frac{ds}{2\pi i} \\ &\leqslant\frac{\pi^2h^2}{4\sqrt{d}}\int_{\frac{3}{2}+\varepsilon-i\infty}^{\frac{3}{2}+\varepsilon+i\infty}4^{s+\varepsilon}M^{s+\varepsilon+\frac{1}{2}}\Gamma\left(s+\varepsilon+\frac{1}{2}\right)^2 \\ &\quad\cdot\frac{s^2\left(s-\frac{1}{2}\right)^{-3}}{(s-1-\varepsilon)(s-1+\varepsilon)}\frac{ds}{2\pi i},\end{aligned}$$

$$\leqslant\frac{\pi^2h^2}{4\sqrt{d}}\left(4^{s+\varepsilon}M^{s+\varepsilon+\frac{1}{2}}\Gamma\left(s+\varepsilon+\frac{1}{2}\right)^2\frac{4}{\varepsilon}\right)\bigg|_{s=1},$$

由此即得

$$J_3\leqslant\frac{4\pi^2h^2}{\sqrt{d}}M^{\frac{3}{2}}\Gamma\left(\frac{3}{2}+\varepsilon\right)\frac{(4M)^\varepsilon}{\varepsilon},\tag{5.131}$$

取

$$\varepsilon^{-1}=\max\{2,\ \log(4M)\},\tag{5.132}$$

则有

$$\Gamma\left(\frac{3}{2}+\varepsilon\right)\leqslant\Gamma(2)=1,\ (4M)^\varepsilon\leqslant e,$$

再由(5.131)与(5.132)可得

$$J_3\leqslant\frac{h^2}{\sqrt{d}}4\pi^2eM^{\frac{3}{2}}\max\{2,\ \log(4M)\}$$
$$\leqslant\frac{h^2}{\sqrt{d}}4\pi^2eM^{\frac{3}{2}}\log(4M),\tag{5.133}$$

其中用到 $4M=N\pi^{-2}$ 或 $\sqrt{N}\pi^{-2}$。由(5.123)、(5.129)、(5.130)和(5.133)有下面的引理。

引理 3.7 设 c_1, c_2, c_3 如(5.116)和(5.119)所示，是与 d 无关的常数(c_1, $c_3>0$)。则有

$$\left|c_1G(U,\ 1)\left(\log d+\frac{G'(U,\ 1)}{G(U,\ 1)}+c_2\right)\right|\leqslant c_3\sup_{s\in\Gamma}|G(U,\ s)|$$
$$+\frac{M}{96}\frac{h^2}{\sqrt{U}}\left(3.3+\left|\log\frac{dM}{U}\right|\right)^4+\frac{h^2}{\sqrt{d}}4\pi^2eM^{\frac{3}{2}}\log(4M)$$
$$+\frac{2\pi^4}{3}M^{\frac{3}{2}}h\sum_{q\in\mathfrak{A}}a(q)^{-1}.$$

证明 除已指出的各式以外，再注意到(5.113)。(5.114)与(5.118)即得所需。

3.4 GGZO 定理的证明(三)

本小节中，沿用以上各小节的记号，特别已设 $d>4$。

引理 3.8 我们有

$$1\leqslant\sum_{q\in\mathfrak{A}}a(q)^{-1}\leqslant\alpha_1\prod_{p\in P(d)'}\left(1+\frac{1}{p}\right),$$

这里 $P'(d)$ 表示在 $P(d)$ 中去掉那些大于等于 U 的素数，而

$$\alpha_1=\left(1+\frac{h}{U}\right)\left(\frac{1+V^{-1}}{1-V^{-1}}\right),\ V=\left(\frac{d}{4}\right)^{\frac{1}{h}}.$$

证明 命 $a=a(q)$，$b=b(q)$，$c=c(q)$ 为 $q(x,y)=ax^2+bxy+cy^2$ 的三个系数，这里 $q\in\mathfrak{B}$。那么有 $4ac-b^2=d$。

于是 a 的任一个素因子 p 均满足

$$\chi(p)=\left(\frac{-d}{p}\right)=0 \text{ 或 } 1,$$

这里 $\left(\frac{-d}{*}\right)$ 为 Kronecker 符号，并且可知这时 $\chi(p)=0$ 当且仅当 $p|d$，$\chi(p)=1$ 如 $p\nmid d$，$p|a$。因此可设 a 的标准分解式为

$$a=a(q)=q_1^{n_1}\cdots q_j^{n_j}p_1^{m_1}\cdots p_k^{m_k},$$

其中素数 $q_1,\cdots,q_j$ 均不是 d 的因子，而素数 $p_1,\cdots,p_k$ 均为 d 的因子。

易见 $m_1=\cdots=m_k=1$（此因如有 $p_i^2|d$，则 p_i 只能为 2，此时 $4|d$，且 $-\frac{d}{4}\equiv 0$ 或 $1 \pmod 4$，这是不可能的），注意引理 3.3 已证明 d 的最大素因子 $p_0>U$。

当 $a=a(q)$ 为 d 的某个素因子 p 时，$b=b(q)$ 满足

$$b^2\equiv -d \pmod{4p},\ -p<b\leqslant p,$$

这个同余方程的解数为 1。因此当 $p\in P(d)$ 时，p 对 $\sum_{q\in\mathfrak{B}}a(q)^{-1}$ 所贡献的 p-部分至多为 $1+\frac{1}{p}$。

当 $a=a(q)=q_1^{n_1}$，素数 $q_1\nmid d$ 时，由 $\chi(q_1)=1$ 即知这种 q_1 对 $\sum_{q\in\mathfrak{B}}a(q)^{-1}$ 所贡献的 q_1-部分至多为

$$1+\sum_{n_1=1}^{\infty}\frac{2}{q^{n_1}}=\frac{1+\frac{1}{q_1}}{1-\frac{1}{q_1}}.$$

引理 3.3 已证明小于等于 U 的这种素数 q_1 至多有一个，且 $q_1\geqslant V$。

由上述讨论，即知有

$$\sum_{q\in\mathfrak{A}} a(q)^{-1}\leqslant\frac{1+\frac{1}{V}}{1-\frac{1}{V}}\prod_{p\in P(d)'}\left(1+\frac{1}{p}\right)\cdot\sum_{\substack{q\in\mathfrak{A}\\ p\mid a(q)\Rightarrow p>U}} a(q)^{-1},$$

(5.134)

这里 p 表素数，又易见有

$$\sum_{\substack{q\in\mathfrak{A}\\ p\mid a(q)\Rightarrow p>U}} a(q)^{-1}\leqslant 1+\frac{1}{U}\sum_{q\in\mathfrak{A}}1\leqslant 1+\frac{h}{U}, \qquad (5.135)$$

由(5.134)与(5.135)即得引理。

引理 3.9 记号如上，我们有

$$|G(U,\ 1)|\geqslant\left(\frac{1-V^{-\frac{1}{2}}}{1+V^{-\frac{1}{2}}}\right)^2\prod_{p\in P(d)'}G_p(1).$$

证明 素数 p 满足 $p<U$ 与 $\chi(p)=-1$ 时，$G_p(s)=1$。又满足 $p<U$，$\chi(p)=1$ 的素数 p 至多只有一个，且 $p\geqslant V$，对这一个可能的 p，有

$$|G_p(1)|=\left|\frac{1+\alpha_p p^{-1}}{1-\alpha_p p^{-1}}\right|^2\geqslant\left|\frac{1-V^{-\frac{1}{2}}}{1+V^{-\frac{1}{2}}}\right|^2.$$

这里用了 $|\alpha_p|=\sqrt{p}$；又已知 d 的最大素因子大于等于 U。故得引理。

引理 3.10 记号如上，我们有

$$\sup_{s\in\Gamma}\left|\frac{G(U,\ s)}{G(U,\ 1)}\right|\leqslant\frac{(1+V^{-\frac{1}{2}})^2}{(1-V^{-\frac{1}{4}})^4}\prod_{p\in P(d)}(1-p^{-\frac{1}{4}})^{-2}.$$

证明 可仿照上一引理的证明得出，只要注意 $s\in\Gamma$ 时，有 $\mathrm{Re}s\geqslant 1-\eta$，而 $0<\eta\leqslant\frac{1}{4}$。

引理 3.11 记号如上，我们有

$$\frac{G'(U,\ 1)}{G(U,\ 1)}\geqslant\sum_{p\in P(d)'}\frac{G'_p(1)}{G_p(1)}-\frac{4V^{-\frac{1}{2}}}{1-V^{-1}}\log V.$$

证明 仿照以上两个引理的证明可知，满足 $q_1<U$ 与 $\chi(q_1)=1$ 的素数 q_1 至多只有一个，且 $q_1\geqslant V$。由此

$$\frac{G'(U,1)}{G(U,1)}=\sum_{p\in P(d)'}\frac{G_p'(1)}{G_p(1)}-\frac{\alpha_{q_1}q_1^{-1}\log q_1}{1+\alpha_{q_1}q_1^{-1}}-\frac{\alpha_{q_1}q_1^{-1}\log q_1}{1-\alpha_{q_1}q_1^{-1}}$$
$$-\frac{\bar\alpha_{q_1}q_1^{-1}\log q_1}{1+\bar\alpha_{q_1}q_1^{-1}}-\frac{\bar\alpha_{q_1}q_1^{-1}\log q_1}{1-\bar\alpha_{q_1}q_1^{-1}}$$
$$=\sum_{p\in P(d)'}\frac{G_p'(1)}{G_p(1)}-\frac{2\alpha_{q_1}q_1^{-1}\log q_1}{1-\alpha_{q_1}^2q_1^{-2}}-\frac{2\bar\alpha_{q_1}q_1^{-1}\log q_1}{1-\bar\alpha_{q_1}^2q_1^{-2}},\tag{5.136}$$

再注意到

$$\frac{G'(U,1)}{G(U,1)}=\sum_{p<U}\frac{G_p'(1)}{G_p(1)}$$

的右边的和式中的每一项 $\dfrac{G_p'(1)}{G_p(1)}$ 均为实数，即由(5.136)得出引理，因为有

$$|\alpha_{q_1}|=\sqrt{q_1}\geqslant\sqrt{V}.$$

现在进入 GGZO 定理的最后证明。

由引理 3.7～引理 3.11，可得

$$c_1\left(\frac{1-V^{-\frac12}}{1+V^{-\frac12}}\right)^2\left(\log d+\sum_{p\in P(d)'}\frac{G_p'(1)}{G_p(1)}-\frac{4V^{-\frac12}}{1-V^{-1}}\log V\right.$$
$$\left.+c_2-\frac{c_3}{c_1}\frac{(1+V^{-\frac12})^2}{(1-V^{-\frac14})^4}\prod_{p\in P(d)}(1-p^{-\frac14})^{-2}\right)\prod_{p\in P(d)'}|G_p(1)|$$
$$\leqslant\frac{2\pi^4M^{\frac32}}{3}\left(a_1+\frac{M^{-\frac12}}{64\pi^4}\frac{h}{\sqrt U}\left(3.3+\left|\log\frac{dM}{U}\right|\right)^4\right.$$
$$\left.+\frac{e\log(4M)}{2\pi^2}\frac{h}{\sqrt d}\right)h\prod_{p\in P(d)'}\left(1+\frac1p\right).\tag{5.137}$$

由 Heegner-Baker-Stark 定理知，可设 h⩾2。再命

$$d\geqslant e^{\lambda h},\ \lambda>0.\tag{5.138}$$

命 T 为 d 的不同素因子的个数，由 genus 理论知 $h\geqslant 2^{T-1}$，故得

$$\frac1h\prod_{p\in P(d)}(1-p^{-\frac14})^{-2}\leqslant\frac1h\prod_{1\leqslant j\leqslant\frac{\log h}{\log 2}}(1-p_j^{-\frac14})^{-2},$$

这里 p_j 是第 j 个素数，由此可以证明

$$\frac{1}{h}\prod_{p\in P(d)}(1-p^{-\frac{1}{4}})^{-2}\leqslant 226. \tag{5.139}$$

又

$$\sum_{p\in P(d)'}\frac{G_p'(1)}{G_p(1)}=-\sum_{p\in P(d)'}\frac{(2+a_p)p^{-1}\log p}{1+a_p p^{-1}+p^{-1}}$$
$$\geqslant-\sum_{p\in P(d)'}\frac{2\log p}{\sqrt{p}+1}, \tag{5.140}$$

这里用到整数 $|a_p|\leqslant 2\sqrt{p}$。仿上可以证明

$$\sum_{p\in P(d)'}\frac{2\log p}{\sqrt{p}+1}\leqslant 8\sqrt{2T\log T}+2,$$

故由此及 $T\leqslant 1+\frac{\log h}{\log 2}$，用(5.140)即得

$$\frac{1}{h}\sum_{p\in P(d)'}\frac{G_p'(1)}{G_p(1)}>-7.7. \tag{5.141}$$

再由引理 3.8 与(5.138)有(已设 $h\geqslant 2$)

$$V=\left(\frac{d}{4}\right)^{\frac{1}{h}}\geqslant e^{\lambda-\frac{\log 4}{h}}>e^{\lambda-0.7},$$

这样，当 $\lambda\geqslant 50.7$ 时，有

$$\frac{4V^{-\frac{1}{2}}}{1-V^{-1}}\log V<\frac{200}{e^{25}-e^{-25}}<3\times 10^{-9}, \tag{5.142}$$

与

$$\frac{(1+V^{-\frac{1}{2}})^2}{(1-V^{-\frac{1}{4}})^4}<\frac{(1+e^{-25})^2}{(1-e^{-12.5})^4}<1+2\times 10^{-5}. \tag{5.143}$$

由于 $U=\left(\frac{\sqrt{d}}{2}\right)^{\frac{1}{m}}$, $m\geqslant 1$, 故有

$$d_1\overset{\text{def}}{=\!=}\frac{dM}{U}=2^{\frac{1}{m}}Md^{1-\frac{1}{2m}}\geqslant Me^{\frac{\lambda}{2}h}>3e^{50},\ \text{若 }\lambda\geqslant 50.7,$$

于是，当 $\lambda\geqslant 50.7$ 时，有

$$\frac{M^{-\frac{1}{2}}}{64\pi^4}\frac{h}{\sqrt{U}}\left(3.3+\left|\log\frac{dM}{U}\right|\right)^4$$

$$= \frac{1}{64\pi^4 M} \cdot \frac{h}{\sqrt{d}} \sqrt{d_1} (3.3 + \log d_1)^4$$

$$\geqslant \frac{1}{64\pi^4 \sqrt{M}} h 2^{\frac{1}{2m}} e^{-\frac{\lambda h}{4m}} \left(\left(1 - \frac{1}{2m}\right) \lambda h \right.$$

$$\left. + 3.3 + \log (2^{\frac{1}{m}} M) \right)^4 . \tag{5.144}$$

由定义知，当 $h=4$ 时，$m=\frac{3}{2}$，而当 $h \neq 4$ 时，m 是使 $2m(m+1) \geqslant h$ 成立的最小正整数。即有：

$m=1$，若 $h=1, 2, 3$；$m=\frac{3}{2}$，若 $h=4$；

$$2m(m-1) < h \leqslant 2m(m+1),$$

若 $h \geqslant 5$，此时有 $m \geqslant 2$。

因此我们得到

$$\frac{M^{-\frac{1}{2}}}{64\pi^4} \frac{h}{\sqrt{U}} \left(3.3 + \left| \log \frac{dM}{U} \right| \right)^4 < 6.4 \times 10^{-4}, \text{ 若 } \lambda \geqslant 50.7. \tag{5.145}$$

又由引理(3.8)可知，当 $\lambda \geqslant 50.7$ 时，有

$$\alpha_1 = \left(1 + \frac{h}{U}\right) \left(\frac{1 + V^{-1}}{1 - V^{-1}} \right) = \left(1 + h \left(\frac{d}{4} \right)^{-\frac{1}{2m}} \right) \frac{1 + V^{-1}}{1 - V^{-1}}$$

$$\leqslant (1 + 2^{\frac{1}{m}} h e^{-\frac{\lambda h}{2m}}) \left(\frac{1 + e^{-50}}{1 - e^{-50}} \right),$$

仿照上述办法，利用 m 与 h 的关系可得

$$\alpha_1 \leqslant 1 + 1.87 \times 10^{-11}, \text{ 若 } \lambda \geqslant 50.7, \tag{5.146}$$

最后还可有

$$\frac{e \log(4M)}{2\pi^2} \frac{h}{\sqrt{d}} < 6 \times 10^{-12}, \text{ 若 } \lambda \geqslant 50.7, \tag{5.147}$$

以上用到 $M = \frac{N}{4\pi^2}$ 或 $\frac{\sqrt{N}}{4\pi^2}$，从而有

$$1.8 < M < 129. \tag{5.148}$$

这样由(5.137)—(5.148)可知，当 $h \geqslant 2$ 以及

$$\frac{\log d}{h} \geqslant \lambda \geqslant 50.7 \tag{5.149}$$

时，有

$$\frac{N^{2.5}}{24\tilde{\Lambda}(2)}h \geqslant \left|1-\frac{\alpha}{\lambda}\right|\theta_1(d)\log d, \tag{5.150}$$

这里

$$\alpha = 227\frac{c_3}{c_1}+|c_2|+7.71>0, \tag{5.151}$$

$$\theta_1(d)=\prod_{p\in P(d)'}\frac{|G_p(1)|}{1+p^{-1}}, \tag{5.152}$$

而 c_1, c_2, c_3 如(5.116)与(5.119)所示，与 d 无关，只与所取的椭圆曲线 E/Q(5.53)有关，是可以有效地计算的常数，并且 c_1, $c_3>0$。

对 $p\in P(d)'$，有 $G_p(1)=1+a_p p^{-1}+p^{-1}$，故由(5.152)有

$$\begin{aligned}\theta_1(d) &= \prod_{p\in P(d)'}\frac{|p+1+a_p|}{p+1} \geqslant \prod_{p\in P(d)'}\frac{p+1-[2\sqrt{p}]}{p+1}\\ &= \prod_{p\in P(d)'}\left(1-\frac{[2\sqrt{p}]}{p+1}\right)\\ &\geqslant \prod_{p\in P(d)}\left(1-\frac{[2\sqrt{p}]}{p+1}\right) \overset{\text{def}}{=\!=} \theta(d).\end{aligned} \tag{5.153}$$

经具体而繁复的计算，可以证明 $\alpha<\lambda$，若 $\lambda\geqslant 50.7$。命

$$C=\max\left\{\lambda,\ \left(1-\frac{\alpha}{\lambda}\right)^{-1}\frac{N^{2.5}}{24\tilde{\Lambda}(2)}\right\}. \tag{5.154}$$

这样，由(5.150)—(5.154)即得

$$Ch(-d)\geqslant\theta(d)\log d. \tag{5.155}$$

经过繁复的计算，可以证明可取 $C=55$。这样由 (5.155) 可知 GGZO 定理已完全证明了。至于最后两处所提及的繁复计算，可参见 J.Oesterlé[84]。

本 章 评 注

1. 虚二次域类数 1 问题的解决在当年(1966 年) 曾引起很大反响，在直至 1970 年的四、五年间出现许多论文，包括 C.L.Siegel

等大师，都对这一问题的解法，提出各自的看法。但基本上都与Heegner-Stark-Baker 的方法大同小异。

2. 1971年A. Baker 与H. Stark 又解决了虚二次域的类数2问题，之后似乎看不到进一步的苗头。直至D.Goldfeld 于1975年提出他的明见，这个问题才有所松动，并驱使B. Gross 和D. Zagier 在椭圆曲线方面取得成就，于是于1983年一举解决了虚二次域的Gauss 类数猜想。

3. 本章对椭圆曲线和模形式的介绍是相当粗糙的。有兴趣的读者，除上述所列举的三本书之外，还可参阅参考文献[5]、[26]、[44]、[72]、[73]、[90]、[102]、[109]和[111]等。

4. 本章第三节虽然对GGZO定理的证明作了较系统和全面的介绍，但读者如有兴趣仍可对具体的数值作出改进。

5. 虚二次域的类数虽然已得到有效下界，但距理想境界仍有很大距离，如何进一步改进，这是下一代数学家的任务了。

第 6 章

实二次域的 Gauss 类数猜想

本章中我们将致力于实二次域的 Gauss 类数问题的研究。

Gauss 关于存在无穷多个类数为 1 的实二次域的猜想是一个非常困难的问题，至今还看不到有解决这一问题的任何线索，其中主要的困难在于实二次域的正则子（即基本单位的自然对数）可以说毫无规律可循。由第四章所叙述的 C.L. Siegel 和 Tatuzawa 的工作可知，对一个正则子为 $\log\varepsilon_d$ 的实二次域 $Q(\sqrt{d})$，其类数 $h(d)$ 与其判别式 d 的关系为

$$\log(h(d)\log\varepsilon_d)\sim\frac{1}{2}\log d,\ \text{当}\ d\to+\infty,$$

这里～表示两边的∞是等价的，即它们之比的极限为 1。由这一关系即知为什么正则子如此重要。

我们在第一节中，讨论类数 $h(d)=1$ 的实二次域 $Q(\sqrt{d})$ 的 $\omega\left(=\frac{\sqrt{d}}{2}\text{ 或 }\frac{1+\sqrt{d}}{2}\text{，视 } d \text{ 偶或奇而定}\right)$ 的简单连分数展开式基本周期长度 $p(\omega)$ 的无穷大阶。在第二节中，我们给出 $p(\omega)$ 给定时，实二次域 $Q(\sqrt{d})$ 的类数 $h(d)=1$ 的一系列判别准则，特别对第一章 §2.1 末尾的 10 个例子给出详细的讨论。在第三节中，我们利用第三章中的极限公式，对给定的实二次域，给出有关的虚二次域的一批类数公式。在第四节中，我们详细讨论 S.Chowla 的一个猜想，即猜想只存在六个素数 $p=4N^2+1$（N 为正整数）使实二次域 $Q(\sqrt{p})$ 的类数为 1。在第五节中，我们叙述 D.Goldfeld 的工作，它类似于第五章的 §3，是应用椭圆曲线的有关理论来研究实二次域的类数问题，即假定存在一条其 L 函数在 $s=1$ 处具有 $r(\geqslant 4)$ 阶零点的椭圆模曲线，而来证明对满足 $\log\varepsilon_d\asymp(\log d)^{\delta_0}$（$\asymp$

表示两边的无穷大同阶）的实二次域$Q(\sqrt{d})$的类数$h(d)>c_\delta(\log d)^{r-2-\delta_0-\delta}$，这里$\delta>0$为任给正常数，$c_\delta$为一个仅依赖于$\delta$的可以有效地计算的正常数，因此在$r>2+\delta_0$时，小类数问题可获有效解决。特别是对第四节的S.Chowla猜想，那里的$\log\varepsilon_p\asymp\log p$，这样，如果确能找到一条其$L$函数在$s=1$处具有至少为4阶的零点的椭圆模曲线，则S.Chowla猜想可以完全解决。

§1 实二次域Gauss类数猜想的一般性讨论

1.1 Siegel-Tatuzawa定理的推论

对一个判别式$d_K=d>0$的实二次域$K=Q(\sqrt{d})$，设K的基本单位为$\varepsilon=\varepsilon_K=\varepsilon_d$，$K$的类数$h_K=h_d=h(d)$。则我们有经典的类数公式

$$h_K=\frac{\sqrt{d_K}L(1,\chi_K)}{2\log\varepsilon_K},$$

这里$\chi_K(*)=\chi_d(*)=\left(\frac{d}{*}\right)$是Kronecker符号，$L(1,\chi_K)=\sum_{n=1}^{\infty}\frac{\chi_K(n)}{n}$。

这样由第四章§1.2的Siegel-Tatuzawa定理，我们有下列的两个定理。

定理1.1 $\log(h(d)\log\varepsilon_d)\sim\frac{1}{2}\log d$，当$d\to+\infty$，这里$d$跑过正的基本判别式。

定理1.2 任给满足$0<\delta\leqslant(6\log 10)^{-1}$的正常数$\delta$。再设基本判别式$d\geqslant e^{\frac{1}{\delta}}$，则除去至多有一个例外情况以外，均有

$$h(d)>\min\left\{\frac{0.125}{\log d},\ \frac{14\delta}{d^\delta}\right\}\frac{d^{\frac{1}{2}}}{2\log\varepsilon_d}.$$

由这两个定理，显然可得下列两个推论。

推论 假设存在无穷多个类数$h(d)=1$的实二次域$K=Q(\sqrt{d})$。则当d跑过这些实二次域的判别式而趋向于$+\infty$时，

我们有下列两个结论：

(1) $$\log\log\varepsilon_d \sim \frac{1}{2}\log d, \text{ 当 } d\to+\infty;$$

(2) 对任给的正常数 $\delta>0$，均有

$$\log\varepsilon_d > 7\delta d^{\frac{1}{2}-\delta}, \text{ 若 } d>e^{\frac{7}{\delta}},$$

至多在所考虑的无穷多个实二次域中除去一个可能的例外。

附注 由推论可知欲使实二次域 $K=Q(\sqrt{d})$ 的类数 $h(d)=1$，则必需其正则子 $\log\varepsilon_d$ 的无穷大阶为相当大，如前所示，大约为 $d^{\frac{1}{2}}$。这是很难在实际的计算中实现的，虽然在已计算出的类数表中，类数1的实二次域确实占了相当大的比例。

1.2 简单连分数与类数猜想

在第四章§2中，我们定义了一个实二次域 $K=Q(\sqrt{d})$ 的长度：

$$p(K)=p(Q(\sqrt{d}))=\frac{1}{h(d)}\sum_{A\in\mathscr{C}_K}p(A),$$

这里 d 是 K 的判别式，$h(d)$ 是类数，$\mathscr{C}_K$ 为理想类群，A 跑过 $\mathscr{C}_K$ 中的所有理想类，$p(A)$ 是 A 的长度（定义见第四章§2）。由第四章定理2.1及其附注，可得

定理1.3 当 d 跑过正的基本判别式时，我们有

$$\frac{\log p(Q(\sqrt{d}))}{\log\log\varepsilon_d}\to 1, \text{ 当 } d\to+\infty.$$

这里 $\log\varepsilon_d$ 为 $Q(\sqrt{d})$ 的正则子。

由第四章的定理2.1以及上述的定理1.1—定理1.3，显然可得下列两个定理。

定理1.4 假设存在无穷多个类数 $h(d)=1$ 的实二次域 $K=Q(\sqrt{d})$，则当 d 跑过这些实二次域的判别式而趋向于 $+\infty$ 时，我们有

$$\log p(\alpha_d)\sim\frac{1}{2}\log d, \text{ 当 } d\to+\infty,$$

这里 $p(\alpha_d)$ 是 α_d 的简单连分数展开式基本周期长度，而

$$\alpha_d=\begin{cases}\dfrac{1+\sqrt{d}}{2}, & \text{当 } d \text{ 奇;}\\[2ex] \dfrac{\sqrt{d}}{2}, & \text{当 } d \text{ 偶。}\end{cases}$$

定理 1.5 假设存在无穷多个类数 $h(d)=1$ 的实二次域 $K=Q(\sqrt{d})$，则当 d 跑过这些实二次域的判别式而趋向于 $+\infty$ 时，对任给正常数 $\delta>0$，至多除去一个例外，我们均有

$$p(\alpha_d)>c_\delta d^{\frac{1}{2}-\delta},\quad \text{如 } d\geqslant d_\delta,$$

这里 c_δ 与 d_δ 均为只依赖于 δ 的可以有效地计算的正常数。

问题 对定理 1.5 中的 c_δ 与 d_δ 给出依赖于 δ 的显式。

附注 由定理 1.4 与定理 1.5 可知，对充分大的判别式 d，想要实二次域 $K=Q(\sqrt{d})$ 的类数 $h_K=1$，则 α_d 的简单连分数展开式基本周期的长度必需相当大，例如：

判别式 $d=350240722763374(\approx 3.5\times 10^{14})$ 的实二次域 $K=Q(\sqrt{d})$ 有 $p(\alpha_d)=704007281(\approx 7\times 10^{7})$ 和 $h_K=1$。

对于 $p(\alpha_d)$ 比较小的实二次域 $Q(\sqrt{d})$，由上述定理可知，其中类数等于 1 的域是很少的，这方面最典型的例子是：

S. Chowla 猜想 正好存在六个形如 $p=4N^2+1$ (N 是正整数)的素数，使实二次域 $Q(\sqrt{p})$ 的类数为 1。

我们将在 §4 中详细讨论这一猜想。

§2 实二次域类数为 1 的判别准则

在本节中，我们用连分数给出实二次域类数为 1 的判别准则，然后给出一些典型的例子。

2.1 类数为 1 的一些判别准则

我们的第一个判别准则是下列的定理 2.1。

定理 2.1 设 d 是一个正的基本判别式。实二次域 $K=$

$Q(\sqrt{d})$ 的类数为 $h_K = h(d)$，则有

(1) $\sum_{i=1}^{k} a_i + \theta \leqslant \lambda_1(d) + \lambda_2(d)$;

(2) $h_K = 1$ 当且仅当 $\sum_{i=1}^{k} a_i + \theta = \lambda_1(d) + \lambda_2(d)$,

这里 $\lambda_1(d)$ 与 $\lambda_2(d)$ 分别是下列二个不定方程

$$x^2 + 4yz = d,\ x,\ y,\ z \in \mathbb{Z},\ x,\ y,\ z \geqslant 0;$$

$$x^2 + 4y^2 = d,\ x,\ y \in \mathbb{Z},\ x,\ y \geqslant 0$$

的解数，并设实二次无理数

$$\alpha = \alpha_d = \begin{cases} \dfrac{\sqrt{d}}{2}, & \text{如 } d \text{ 偶;} \\ \dfrac{1+\sqrt{d}}{2}, & \text{如 } d \text{ 奇。} \end{cases}$$

有简单连分数展开式

$$\alpha = [a_0, \overline{a_1, \cdots, a_k}],$$

其中 $\overline{a_1, \cdots, a_k}$ 为基本周期，最后

$\theta = 0$, 如 d 奇, $k = 2n$ (偶数), a_n 奇;

$\theta = 1$, 如 d 奇, $k = 2n$ (偶数), a_n 偶; 或 d 与 k 均奇;

或 d 偶, $k = 2n$ (偶数), a_n 奇;

$\theta = 2$, 其他情况。

附注 这个定理是我们于 1979 年发表的[47]，后来又把它加以改造，成为定理 2.2 的形式，后者实际上与 F. Hirzebruch 和 D. Zagier 的一个结果[33]吻合。我们只给出定理 2.2 的证明。

定理 2.2 设 d 为一个正的基本判别式，在实二次域 $K = Q(\sqrt{d})$ 的理想类群 $\mathscr{C}_K$ 的每一个理想类 A 中选取一下如下的代表

$$\mathfrak{A} = \left[A,\ \frac{\pm B + \sqrt{d}}{2}\right],$$

这里 $A, B, C \in \mathbb{Z}$, $0 \leqslant B \leqslant A \leqslant C$, $B^2 + 4AC = d$。再令

$\alpha_A = \alpha_{\mathfrak{A}} = \dfrac{\pm B + \sqrt{d}}{2A}$ 的简单连分数展开式为

$$\alpha_{\mathbf{A}} = \alpha_{\mathfrak{A}} = [a_0, \overline{a_1, \cdots, a_k}],$$

其中 $\overline{a_1, \cdots, a_k}$ 为基本周期。

则我们有

$$\sum_{\substack{b \in \mathbb{Z}, |b| < \sqrt{d} \\ b \equiv d (\bmod 2)}} \tau\left(\frac{d-b^2}{4}\right) = 2 \sum_{\mathbf{A} \in \mathscr{F}_K} s(\mathbb{A}),$$

这里 $\tau(*)$是 $*$ 的正因子的个数，并在上述记号下

$$s(\mathbb{A}) = s(\alpha_{\mathbf{A}}) = s(\alpha_{\mathfrak{A}}) = \sum_{i=1}^{k} a_i.$$

证明 注意到在定理的假定下，$\mathfrak{A}^* = \left[A, \dfrac{\mp B + \sqrt{d}}{2}\right]$是理想类 $\mathbb{A}^{-1}$ 的代表元，并由第一章引理 1.5 可知，$\alpha_{\mathbf{A}^{-1}}$ 的简单连分数展开式为

$$\alpha_{\mathbf{A}^{-1}} = [a_k - a_0, \overline{a_{k-1}, a_{k-2}, \cdots, a_2, a_1, a_k}],$$

其中 $\overline{a_{k-1}, a_{k-2}, \cdots, a_2, a_1, a_k}$ 为基本周期。由此可知有

$$s(\mathbb{A}^{-1}) = s(\mathbb{A}).$$

考虑第一章引理 1.9 中的集合$\mathfrak{M}$的计数，即知定理 2.2 归结为证明下面的引理 2.1。

引理 2.1 设 d 为一个正的基本判别式，再设有理整数 P, $Q \neq 0$ 使 $\overline{Q} = \dfrac{d-P^2}{4Q} \in \mathbb{Z}$，且使 $\omega = \dfrac{P+\sqrt{d}}{2Q}$ 是一个约化的实二次无理数。最后设 $\mathbb{A}$, $\alpha_{\mathbf{A}}$ 等如上述定理 2.2 所示，则我们有

$$\omega \sim \alpha_{\mathbf{A}} \text{ 当且仅当} \left[Q, \frac{-P+\sqrt{d}}{2}\right] \in \mathbb{A}^{-1}.$$

证明 $\omega \sim \alpha_{\mathbf{A}}$ 即 ω 相似于 $\alpha_{\mathbf{A}}$，也即存在 $r, u, s, t \in \mathbb{Z}$, $ru - st = \delta = \pm 1$，使 $\omega = \dfrac{r\alpha_{\mathbf{A}} + s}{t\alpha_{\mathbf{A}} + u}$。由此易得

$$\delta Q = Au^2 \pm But - Ct^2,$$

$$\delta P = 2Aus \pm B(ru + st) - 2Crt,$$

$$-\delta \overline{Q} = As^2 \pm Bsr - Cr^2.$$

因此当 $\delta = 1$ 时，即 $ru - st = 1$ 时，有

$$((Q, P, -\overline{Q})) \approx ((A, \pm B, -C)), \tag{6.1}$$

再考虑到 ω 为约化的以及 A, B, C 的性质，可知

$((Q,\ P,\ -\bar{Q}))$为属于理想$\left[Q,\ \frac{-P+\sqrt{d}}{2}\right]$的二次型,

$((A,\ \pm B,\ -C))$为属于理想$\left[A,\ \frac{\mp B+\sqrt{d}}{2}\right]$的二次型,

由此及 (6.1), 用第二章的引理 2.1, 可得 $\left[Q,\ \frac{-P+\sqrt{d}}{2}\right]\approx \mathfrak{A}^*$, 即有$\left[Q,\ \frac{-P+\sqrt{d}}{2}\right]\in \mathbb{A}^{-1}$。

而当 $\delta=-1$ 时, 即 $ru-st=-1$ 时, 令 $u_1=-u$, $s_1=-s$, 即有 $u_1r-s_1t=1$, 及

$$((Q,\ P,\ -\bar{Q}))\overset{\binom{u_1 t}{s_1 r}}{\approx}((-A,\ \pm B,\ C)),$$

于是$((Q,\ P,\ -\bar{Q}))\sim((A,\ \pm B,\ -C))$, 同上可得 $\left[Q,\ \frac{-P+\sqrt{d}}{2}\right]\sim\mathfrak{A}^*$, 如以第二章的引理 2.2 代替该章的引理 2.1。这样仍可得到$\left[Q,\ \frac{-P+\sqrt{d}}{2}\right]\in \mathbb{A}^{-1}$。

反之, 把上述证明过程反过来, 即可证明当$\left[Q,\ \frac{-P+\sqrt{d}}{2}\right]\in \mathbb{A}^{-1}$时, 必有 $\omega\sim\alpha_{\mathbb{A}}$。

引理得证, 从而定理 2.2 也随之成立。

附注 (1) 在引理 2.1 的证明过程中可以看出

$$\omega\approx\alpha_{\mathbb{A}}\Longleftrightarrow\left[Q,\ \frac{-P+\sqrt{d}}{2}\right]\approx \mathbb{A}^{-1},$$

这里左边的"≈"是实二次无理数之间的严格相似, 右边的"≈"是理想类之间的严格相似。

(2) 由定理 2.2 不难证明定理 2.1, 详细过程不叙述了。

定理 2.2 可以推广为下列的定理 2.3。

定理 2.3 设 $f(x)$是 x 的任一个给定的函数, 则在定理 2.2 的记号下, 我们有

$$\sum_{\substack{b\in\mathbb{Z},\,|b|<\sqrt{d}\\ b\equiv u\,(\mathrm{mod}\,2)}}\ \sum_{\substack{1<a\in\mathbb{Z}\\ a\,\mid\,\frac{d-b^2}{4}}} f(a)=\sum_{\mathbb{A}\in\wp_K} s_f(\mathbb{A}),$$

这里

$$s_f(A)=\sum_{n=1}^{k}\sum_{t=1}^{a_n}(f(Q_n)+f(Q_{n+1}+tP_{n+1}-t^2Q_n)),$$

其中

$$\frac{P_n+\sqrt{d}}{2Q_n}=[a_n,\ a_{n+1},\ \cdots](n\geqslant 0)$$

是 α_A 的第 n 个完全商。

证明　同定理2.2的证明一样，我们考虑第一章引理1.9中的集合$\mathfrak{M}$。对$\mathfrak{M}$中的每个数$\frac{P+\sqrt{d}}{2Q}$，赋予值$f(Q)+f(\hat{Q})$，这里 $\hat{Q}=\frac{d-(P-2Q)^2}{4Q}\in\mathbb{Z}$。由那里的结论有

$$P=2Q_{n+1}-P_{n+1}+2t(P_{n+1}+Q_n)-2t^2Q_n,$$
$$Q=Q_{n+1}+tP_{n+1}-t^2Q_n,$$
$$1\leqslant t\leqslant a_n,\ 1\leqslant n\leqslant k,$$

如 $\frac{P+\sqrt{d}}{2Q}\sim-\alpha'_A$($\alpha'_A$ 是 α_A 的共轭元)，并且易见这时有 $\hat{Q}=Q_n$。由此及上述引理2.1即知，定理2.3归结为证明下列的引理2.2。

引理2.2　设$\mathfrak{M}$如第一章引理1.9所示，则有

$a,\ b\in\mathbb{Z},\ a\geqslant 1,\ |b|<\sqrt{d},\ a\left|\frac{d-b^2}{4}\right.\Rightarrow 1+\frac{b+\sqrt{d}}{2a}$ 或 $1+\frac{2a}{b+\sqrt{d}}\in\mathfrak{M}$，反之，当$\frac{P+\sqrt{d}}{2Q}\in\mathfrak{M}$时，必有 $|P-2Q|<\sqrt{d}$ 且 $Q,\ \hat{Q}=\frac{d-(P-2Q)^2}{4Q}\geqslant 1$。

证明　第二个断言显然成立，以下证明第一个断言。现设

$$a,\ b\in\mathbb{Z},\ a\geqslant 1,\ |b|<\sqrt{d},\ a\left|\frac{d-b^2}{4}\right..$$

令 $a'\in\mathbb{Z}$，使 $d=b^2+4aa'$，则 $a'\geqslant 1$。易见

当 $a>\frac{\sqrt{d}-b}{2}$ 时，$1+\frac{b+\sqrt{d}}{2a}=\frac{b+2a+\sqrt{d}}{2a}\in\mathfrak{M}$；

当 $a<\frac{\sqrt{d}-b}{2}$ 时，$a'>\frac{\sqrt{d}+b}{2}$，

故

$$1+\frac{2a}{\sqrt{d}+b}=1+\frac{-b+\sqrt{d}}{2a'}\in\mathfrak{M}.$$

引理得证。

从而定理 2.3 随之成立。

定理 2.4 在定理 2.3 的记号下，我们有

$$60\zeta_{\mathbb{K}}(-1)=\sum_{\mathbf{A}\in\mathscr{P}_{\mathbb{K}}}\sum_{n=1}^{k}\sum_{t=1}^{a_n}(Q_n+Q_{n+1}+tP_{n+1}-t^2Q_n),$$

这里 $\zeta_{\mathbb{K}}$ 是实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的 Dedekind ζ-函数。

证明 在定理 2.3 中取 $f(x)=x$，即知定理 2.4 归结为证明等式

$$60\zeta_{\mathbb{K}}(-1)=\sum_{\substack{b\in\mathbb{Z},|b|<\sqrt{d}\\ b\equiv d(\mathrm{mod}\,2)}}\sigma\left(\frac{d-b^2}{4}\right),\tag{6.2}$$

这里 $\sigma(*)$ 为 $*$ 的正因子的和。(6.2) 即为 C.L.Siegel[93] 一条定理的内容，故定理 2.4 已证。

定理 2.5 令 $\chi(*)=\left(\frac{-4}{*}\right)$ 为 Kronecker 符号，则在定理 2.3 的记号下有：

$$\sum_{\mathbf{A}\in\mathscr{P}_{\mathbb{K}}}\sum_{n=1}^{k}\sum_{t=1}^{a_n}(\chi(Q_n)+\chi(Q_{n+1}+tP_{n+1}-t^2Q_n))$$

$$=\begin{cases}h(-d), & \text{如 } d\equiv1(\mathrm{mod}\,4);\\ 3h(-d), & \text{如 } d\equiv8(\mathrm{mod}\,16);\\ 6h(-d), & \text{如 } d\equiv12(\mathrm{mod}\,32),\ \text{且 } d>12,\end{cases}$$

这里 $h(-d)$ 是虚二次域 $\mathbb{Q}(\sqrt{-d})$ 的类数。

证明 在定理 2.3 中取 $f(x)=\chi(x)$，即知本定理中等式的左端等于

$$S=\sum_{\substack{b\in\mathbb{Z},|b|<\sqrt{d}\\ b\equiv d(\mathrm{mod}\,2)}}\sum_{\substack{1\leqslant a\in\mathbb{Z}\\ a\mid\frac{d-b^2}{4}}}\chi(a)=\frac{1}{4}\sum_{\substack{b\in\mathbb{Z},|b|<\sqrt{d}\\ b\equiv d(\mathrm{mod}\,2)}}r_2\left(\frac{d-b^2}{4}\right),$$

这里 $r_2(n)$ 是表 n 为二个有理整数的平方和的表法数，这可参考华罗庚著《数论导引》第六章 §7 的定理 2。于是有

$$S=\frac{1}{4}\sum_{\substack{x,y,z\in\mathbb{Z}\\ x^2+4y^2+4z^2=d}}1=\begin{cases}\frac{1}{4}r_3\left(\frac{d}{4}\right), & \text{当 } 4\mid d;\\ \frac{1}{12}r_3(d), & \text{当 } d\equiv1(\mathrm{mod}\,4),\end{cases}$$

这里 $r_3(n)$ 是表 n 为三个有理整数的平方和的表法数，并注意 d 是一个正的基本判别式。由此，再用上述华罗庚著作的 $p.232$ 的结果，即知定理成立，因为这时有

$r_3\left(\frac{d}{4}\right)=12h(-d)$，如 $\frac{d}{4}\equiv 2 \pmod 4$；

$r_3\left(\frac{d}{4}\right)=24h(-d)$，如 $\frac{d}{4}\equiv 3 \pmod 8$，且 $d>12$；

$r_3(d)=12h(-d)$，如 $d\equiv 1 \pmod 4$。

定理证毕。

由上述的各个定理，我们可以得到下列几个判别准则：

判别准则 A　判别式为 d 的实二次域 $Q(\sqrt{d})$ 的类数为 1 的充要条件是

$$\sum_{\substack{b\in \mathbb{Z},\,|b|<\sqrt{d}\\ b\equiv d(\bmod 2)}} \tau\left(\frac{d-b^2}{4}\right)=2\sum^{k} a_n,$$

这里 $\tau(m)$ 是 m 的正因子的个数，且 $\alpha=\frac{\sqrt{d}}{2}$ 或 $\frac{1+\sqrt{d}}{2}$（视 d 偶或奇而定）的简单连分数展开式为

$$\alpha=[a_0, \overline{a_1, \cdots, a_k}],$$

其中 $\overline{a_1, \cdots, a_k}$ 为基本周期。

证明　这由定理 2.2 即得。

判别准则 B　判别式为 d 的实二次域 $K=Q(\sqrt{d})$ 的类数为 1 的充要条件是

$$60\zeta_K(-1)=\sum^{k}\left(a_nQ_{n+1}+\frac{a_n(a_n^2+5)}{6}Q_n\right),$$

这里 ζ_K 为 K 的 Dedekind ζ-函数，而且 $\alpha=\frac{\sqrt{d}}{2}$ 或 $\frac{1+\sqrt{d}}{2}$（视 α 偶或奇而定）的简单连分数展开式为

$$\alpha=[a_0, \overline{a_1, \cdots, a_k}],$$

其中 $\overline{a_1, \cdots, a_k}$ 为基本周期，α 的第 n 个完全商为

$$[a_n, a_{n+1}, \cdots]=\frac{P_n+\sqrt{d}}{2Q_n}\quad (n\geq 0).$$

证明　这由定理 2.4 可得，其中应注意到，据第一章的引理

1.1 与引理 1.3 有

$$a_n=a_{k-n},\ Q_n=Q_{k-n},\ P_n=P_{k+1-n}\ (1\leqslant n\leqslant k-1),\qquad (6.3)$$

$$P_{n+1}+P_n=2a_nQ_n(n\geqslant 0),\ P_{k+1}=P_k=P_1,\qquad (6.4)$$

由此及定理 2.4 即知 $\mathbb{K}$ 的类数为 1 的充要条件为

$$\begin{aligned}60\zeta_{\mathbb{K}}(-1)&=\sum^{k}\sum_{t=1}^{a_n}(Q_n+Q_{n+1}+tP_{n+1}-t^2Q_n)\\&=\sum^{k}\Bigl(a_n(Q_n+Q_{n+1})+\frac{a_n(a_n+1)}{2}P_{n+1}\\&\qquad-\frac{a_n(1+a_n)(1+2a_n)}{6}Q_n\Bigr),\end{aligned}$$

注意到由(6.3)和(6.4)有

$$\begin{aligned}\sum^{k}\frac{a_n(1+a_n)}{2}P_n&=\sum^{k-1}\frac{a_{k-n}(1+a_{k-n})}{2}P_{k-n+1}+\frac{a_k(1+a_k)}{2}P_k\\&=\sum^{k}\frac{a_n(1+a_n)}{2}P_{n+1}=\sum^{k}\frac{a_n(1+a_n)}{2}\Bigl(\frac{P_n+P_{n+1}}{2}\Bigr)\\&=\sum^{k}\frac{a_n^2(1+a_n)}{2}Q_n,\end{aligned}$$

即可得到所欲证明的结论。

2.2 一些典型的例子

现在我们对第一章 §2.1 末尾列举的十个例子(他们是最典型的),给出相应的实二次域类数为 1 的判别准则,即有下列几个定理。

定理 2.6 设无平方因子正整数 $d=4N^2+1$,这里正整数 $N>1$,设实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的类数为 $h_{\mathbb{K}}$,则有

(1) $h_{\mathbb{K}}=1$ 当且仅当 d、N 以及 $N^2-x-x^2(x=1,2,\cdots,N-2)$ 均为素数;

(2) $h_{\mathbb{K}}=1$ 当且仅当小于 N 的有理素数 q 均在 $\mathbb{K}$ 中为惯性的;

(3) $h_{\mathbb{K}}=1$ 当且仅当 $\zeta_{\mathbb{K}}(-1)=\dfrac{N(2N^2+7)}{90}$,其中 $\zeta_{\mathbb{K}}$ 为 $\mathbb{K}$ 的 Dedekind ζ-函数;

(4) 如 $h_K=1$，则虚二次域 $Q(\sqrt{-d})$ 的类数 $h(-d)=2N+4\left(\frac{-4}{N}\right)$，这里 $\left(\frac{-4}{*}\right)$ 为 Kronecker 符号。

证明 (1) 注意此时 $\alpha=\frac{1+\sqrt{d}}{2}$，$\alpha$ 的简单连分数展开式，由第一章 §2.1 知道，有如下表：

n	0	1	2	3
a_n	N	1	1	$2N-1$
P_n	1	$2N-1$	1	$2N-1$
Q_n	1	N	N	1

基本周期长度 $k=3$，故 $s(\alpha)=2N+1$。由判别准则 A 可知 $h_K=1$ 的充要条件是

$$2N+1=\sum_{x=0}^{N-1}\tau(N^2-x-x^2), \tag{6.5}$$

这里 $\tau(n)$ 是 n 的正因子的个数。容易知道 (6.5) 成立的充要条件是 $N^2-x-x^2(1\leqslant x\leqslant N-1)$ 均为素数（注意已设 $N\geqslant 2$），再由 genus 理论即得所需。

附注 由判别准则 $A(1)$ 及上述证明可知，对无平方因子正整数 $d=4N^2+1$（正整数 $N>1$），为使 $Q(\sqrt{d})$ 的类数为 1 必需且只需 $N^2-x-x^2(1\leqslant x\leqslant N-1)$ 均为素数。指出 d 为素数及特别指出 N 为素数是类数为 1 的必要条件，前者是为了更明确些，后者仅仅为了特别指出。这样我们得到了绪论所说的命题 B。

(2) 设 $h_K=1$，如 N 偶，则由 (1) 可知必有 $N=2$，没有可证的。如 N 奇，对 $q=2$，由于 $d=4N^2+1\equiv 5(\bmod 8)$，故 Kronecker 符号 $\left(\frac{d}{2}\right)=-1$，即 2 在 K 中为惯性的。对一个奇素数 $q<N$，如有：Kronecker 符号 $\left(\frac{d}{q}\right)=1$，则定义可知，同余方程

$$y^2\equiv d(\bmod q) \tag{6.6}$$

有解。不妨设正奇数 $y=2x+1\leqslant q$，而 y 满足 (6.6)。即有

$$N^2-x-x^2\equiv 0(\bmod q),\ 0\leqslant x\leqslant\frac{q-1}{2}<\frac{N-1}{2}, \tag{6.7}$$

但当 $1\leqslant x\leqslant N-1$ 时, N^2-x-x^2 是素数, 又 $1\leqslant x<\frac{N-1}{2}$ 时, $N^2-x-x^2>\frac{3N^2+1}{4}>N>q$, 故由(6.7)即知, 只可能 $x=0$. 因此 $q|N^2$. 但 N 为素数, 只可能 $q=N$, 这与 $q<N$ 矛盾. 这说明, 小于 N 的奇素数 q 满足: Kronecker 符号 $\left(\frac{d}{q}\right)=-1$, 即 q 在 $\mathbb{K}$ 中惯性, 总之证明了: $h_{\mathbb{K}}=1$ 时, 小于 N 的素数均在 $\mathbb{K}$ 中惯性.

反之, 设小于 N 的素数均在 $\mathbb{K}$ 中惯性. 我们来证明, 对任意的 $x=1, 2, \cdots, N-1$, N^2-x-x^2 均表素数. 用反证法, 如果有一个有理整数 x_0, $1\leqslant x_0\leqslant N-1$, 使 $N^2-x_0-x_0^2$ 不是素数. 由于 $N^2-x_0-x_0^2>1$, 故可令 q 为 $N^2-x_0-x_0^2$ 的最小素因子, 那么有

$$N^2-x_0-x_0^2=nq,\ n\geqslant q.$$

由此即有 $q<N$, 且有

$$d\equiv(2x_0+1)^2(\mathrm{mod}\ q),$$

从而 Kronecker 符号 $\left(\frac{d}{q}\right)=0$ 或 1, 这与小于 N 的素数均在 $\mathbb{K}$ 中惯性的假设矛盾. 所以由 (1) 即知 $h_{\mathbb{K}}=1$. (2) 得证.

(3) 由判别准则 B 及 (1) 中关于 α 的简单连分数展开式的描述, 即知(注意 $Q_4=Q_1$):

$$h_{\mathbb{K}}=1 \text{ 当且仅当 } 60\zeta_{\mathbb{K}}(-1)=\sum^{3}\left(a_nQ_{n+1}+\frac{a_n(5+a_n^2)}{6}Q_n\right)$$

$$=(2N-1+3)N+1+\frac{(2N-1)(5+(2N-1)^2)}{6}=\frac{N}{3}(4N^2+14N),$$

即 $\zeta_{\mathbb{K}}(-1)=\frac{N(2N^2+7)}{90}$.

(4) 由上一小节的定理 2.5 即知, 如 $h_{\mathbb{K}}=1$, 则 $h(-d)$

$$=\left(\frac{-4}{Q_1}\right)+\left(\frac{-4}{Q_2+P_2-Q_1}\right)+\left(\frac{-4}{Q_2}\right)+\left(\frac{-4}{Q_3+P_3-Q_2}\right)$$

$$+(2N-1)\left(\frac{-4}{Q_3}\right)+\sum_{t=1}^{2N-1}\left(\frac{-4}{Q_1+tP_1-t^2Q_3}\right),$$ 这里 $\left(\frac{-4}{*}\right)$ 为 Kronecker 符号.

于是 $h(-d)=2N+3\left(\frac{-4}{N}\right)+\sum_{t=1}^{2N-1}\left(\frac{-4}{N+(2N-1)t-t^2}\right)=2N+4\left(\frac{-4}{N}\right)$，最后等式可分别对 $N=2$ 及 $N\equiv 1$ 或 $3(\mathrm{mod}4)$ 进行讨论而得出. 故(4)获证。总之，定理已明。

附注 本定理的诸结果是作者首先证明的，以后 A.Mollin 等人又重复了其中的一部分。

用同样的方法，可以证明下列定理，但我们不给出证明。

定理 2.7 对无平方因子正整数 $d=(2N+1)^2+4$, 其中正整数 $N>1$, 设实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的类数为 $h_{\mathbb{K}}$, 则有

(1) $h_{\mathbb{K}}=1$ 当且仅当 d、$2N+1$ 与 $N^2+N+1-x-x^2(0\leqslant x\leqslant N-2)$ 均为素数;

(2) $h_{\mathbb{K}}=1$ 当且仅当小于 $2N+1$ 的素数均在 $\mathbb{K}$ 中惯性;

(3) $h_{\mathbb{K}}=1$ 当且仅当 $90\zeta_{\mathbb{K}}(-1)=(2N+1)(N^2+N+3)$;

(4) 如 $h_{\mathbb{K}}=1$, 则虚二次域 $\mathbb{Q}(\sqrt{-d})$ 的类数 $h(-d)=2N+1+(-1)^N$。

定理 2.8 对无平方因子正整数 $d_0=(2N+1)^2-2$, 其中正整数 $N\geqslant 1$, $d=4d_0$ 是一个正的基本判别式, 设实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的类数为 $h_{\mathbb{K}}$, 则

(1) $h_{\mathbb{K}}=1$ 当且仅当 $d_0, 4N^2+4N-1-4x^2(1\leqslant x\leqslant N)$ 与 $2N^2+2N-1-2x-2x^2(0\leqslant x\leqslant N-1)$ 均为素数;

(2) $h_{\mathbb{K}}=1$ 当且仅当小于 $4N-1$ 的奇素数均在 $\mathbb{K}$ 中惯性;

(3) $h_{\mathbb{K}}=1$ 当且仅当 $\zeta_{\mathbb{K}}(-1)=\frac{N(N+1)(2N+1)}{9}$。

定理 2.9 对无平方因子正整数 $d_0=4N^2-2$, 其中 N 为一个正偶数, $d=4d_0$ 是一个正的基本判别式, 设实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的类数为 $h_{\mathbb{K}}$, 则有

(1) $h_{\mathbb{K}}=1$ 当且仅当 $2N^2-1-2x^2(0\leqslant x\leqslant N-1)$ 与 $4N^2-3-4x-x^2(0\leqslant x\leqslant N-1)$ 均为素数;

(2) $h_{\mathbb{K}}=1$ 当且仅当 $<4N-3$ 的奇素数均在 $\mathbb{K}$ 中惯性;

(3) $h_{\mathbb{K}}=1$ 当且仅当 $18\zeta_{\mathbb{K}}(-1)=N(4N^2-1)$;

定理 2.10 对无平方因子正整数 $d_0=(2N+1)^2+2$, 其中 N 为正整数, $d=4d_0$ 为一个正的基本判别式, 设实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的类数为 $h_{\mathbb{K}}$, 则有

(1) $h_{\mathbb{K}}=1$ 当且仅当 $(2N+1)^2+2-2x^2(0\leqslant x\leqslant N)$ 与 $2N^2+2N+1-2x-2x^2(0\leqslant x\leqslant N-1)$ 均为素数;

(2) $h_{\mathbb{K}}=1$ 当且仅当小于 $4N+1$ 的奇素数均在 $\mathbb{K}$ 中惯性;

(3) $h_{\mathbb{K}}=1$ 当且仅当 $36\zeta_{\mathbb{K}}(-1)=(2N+1)((2N+1)^2+5)$;

(4) 如 $h_{\mathbb{K}}=1$, 则虚二次域 $\mathbb{Q}(\sqrt{-d})$ 的类数

$$h(-d)=\frac{2N+1}{3},$$

从而必有 $N\equiv1(\mathrm{mod}3)$.

定理 2.11 对无平方因子正整数 $d_0=4N^2+2$, 其中 N 是一个正奇数, $d=4d_0$ 是一个正的基本判别式, 设实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的类数为 $h_{\mathbb{K}}$, 则有

(1) $h_{\mathbb{K}}=1$ 当且仅当 $2N^2+1-2x^2(0\leqslant x\leqslant N-1)$ 与 $4N^2+2-(2x+1)^2(0\leqslant x\leqslant N-1)$ 均为素数;

(2) $h_{\mathbb{K}}=1$ 当且仅当小于 $4N-1$ 的奇素数均在 $\mathbb{K}$ 中惯性;

(3) $h_{\mathbb{K}}=1$ 当且仅当 $18\zeta_{\mathbb{K}}(-1)=N(4N^2+5)$;

(4) 如 $h_{\mathbb{K}}=1$, 则虚二次域 $\mathbb{Q}(\sqrt{-d})$ 的类数 $h(-d)=2N$.

定理 2.12 对无平方因子正整数 $d=(2N+1)^2-4$, 其中 N 为一个正偶数, 设实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的类数为 $h_{\mathbb{K}}$, 则有

(1) $h_{\mathbb{K}}=1$ 当且仅当 $2N+3$ 与 $N^2+N-1-x-x^2(0\leqslant x\leqslant N-1)$ 均为素数(充分条件中可去掉 $2N+3$ 为素数的要求);

(2) $h_{\mathbb{K}}=1$ 当且仅当 $<2N-1$ 的素数均在 $\mathbb{K}$ 中惯性;

(3) $h_{\mathbb{K}}=1$ 当且仅当 $90\zeta_{\mathbb{K}}(-1)=N(N+1)(2N+1)$;

(4) 如 $h_{\mathbb{K}}=1$, 则虚二次域 $\mathbb{Q}(\sqrt{-d})$ 的类数 $h(-d)=2N$.

定理 2.13 对无平方因子正整数 $d=4N^2-R$, 其中正整数 $R\equiv3(\mathrm{mod}4)$, $N=MR>3$, M 也是一个正整数, 设实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的类数为 $h_{\mathbb{K}}$, 则有

(1) $h_{\mathbb{K}}=1$ 当且仅当 $4M^2R-1$, R, $N+\frac{R+1}{4}$, M^2R-

$\frac{R+1}{4}-Rx-Rx^2(0\leqslant x\leqslant M-1)$ 与 $N^2-\frac{R+1}{4}-R^2x^2+R(2y+1)x-y-y^2\left(1\leqslant x\leqslant M,\ 0\leqslant y\leqslant R-1,\ y\neq\frac{R-1}{2},\ (x,y)\neq\left(1,\ \frac{3R-1}{4}\right)\right)$ 均为素数(充分条件中可去掉 $4M^2R-1$ 为素数的条件);

(2) $h_K=1$ 当且仅当小于 $N-\frac{R+1}{4}$ 且与 d 互素的素数均在 K 中惯性;

(3) $h_K=1$ 当且仅当 $360\zeta_K(-1)=M(8M^2R^3-3R^2+(8M^2+50)R-3)$(这个结论在 $N=MR=3$ 时也成立);

(4) 如 $h_K=1$, 则虚二次域 $Q(\sqrt{-d})$ 的类数 $h(-d)=2M\cdot(R-1)-(3-(-1)^M)\left(\left(\frac{-4}{M+R_1}\right)+\left(\frac{-4}{M-R_1}\right)\right)$, 这里 $R_1=\frac{R+1}{4}$, $\left(\frac{-4}{*}\right)$是 Kronecker 符号.

定理 2.14 对无平方因子正整数 $d=(2N+1)^2+4R$, 其中 N, R 均为正整数, $R\equiv3\pmod4$, $2N+1=MR$, M 也是正整数, 设实二次域 $K=Q(\sqrt{d})$ 的类数为 h_K, 则有

(1) $h_K=1$ 当且仅当 R, M^2R+4, $x(M-x)R+1\left(1\leqslant x\leqslant\frac{M-1}{2}\right)$ 与 $N^2+N+R-x-x^2(1\leqslant x\leqslant N-1,\ x\not\equiv0\pmod R)$ 均为素数(充分条件中可去掉 M^2R+4 为素数的要求);

(2) $h_K=1$ 当且仅当小于 $2N+2-R(=(M-1)R+1)$ 且与 d 互素的素数均在 K 中惯性;

(3) $h_K=1$ 当且仅当 $360\zeta_K(-1)=M((R^3+R)M^2+6R^2+10R+6)$;

(4) 如 $h_K=1$, 则虚二次域 $Q(\sqrt{-d})$ 的类数 $h(-d)=M(R-1)+2\left(\frac{-4}{M}\right)$, 这里$\left(\frac{-4}{M}\right)$是 Kronecker 符号.

定理 2.15 对无平方因子正整数 $d=(2N+1)^2-4R$, 其中

N, R 均为正整数, $R\equiv 3(\bmod 4)$, $2N+1=MR$, M也是一个正整数, $M>1$, 设实二次域 $K=Q(\sqrt{d})$ 的类数为 h_K, 则有

(1) $h_K=1$ 当且仅当 R,

$$M^2R-4,\ x(M-x)R-1\left(1\leqslant x\leqslant\frac{M-1}{2}\right)$$

与 $N^2+N-R-x-x^2(1\leqslant x\leqslant N-1,\ x\not\equiv 0(\bmod R))$ 均为素数(充分条件中可去掉 M^2R-4 为素数的要求);

(2) $h_K=1$ 当且仅当 $<2N-R$ 且与 d 互素的素数均在 K 中惯性;

(3) $h_K=1$ 当且仅当 $360\zeta_K(-1)=M((R^3+R)M^2-6R^2+10R-6)$;

(4) 如 $h_K=1$, 则虚二次域 $Q(\sqrt{-d})$ 的类数 $h(-d)=2N+1-M-2\left(\frac{-4}{M}\right)$, 这里$\left(\frac{-4}{M}\right)$是 Kronecker 符号.

§3 用连分数表示虚二次域的类数

在 §2 中, 我们已看到虚二次域的类数可以用有关连分数的一些量来表示. 本节中我们给出非常一般的公式, 首先是 F.Hirzebruch-D.Zagier 类数公式, 然后, 我们再给出三个公式, 最后讨论一些例子.

3.1 F.Hirzebruch-D.Zagier 类数公式

下面我们要用 genus 理论中的一些语言, 这可见之于第二章.

定理 3.1 (F.Hirzebruch-D.Zagier)

设 d 为一个正的基本判别式, 实二次域 $K=Q(\sqrt{d})$ 的理想类群与类数分别记为 $\mathscr{C}_K$ 与 h_K. 对每一个理想类 $A\in\mathscr{C}_K$, 可取它的一个代表理想 $\mathfrak{A}=\left[a,\ \frac{-b+\sqrt{d}}{2}\right]$, 使 a, $b\in\mathbb{Z}$, 且 $a>0$,

$g.c.d.(a, d)=1$, $\frac{b^2-d}{4a}\in\mathbb{Z}$。设$\chi$为$\mathscr{C}_{\mathbb{K}}$的一个genus奇特征，即存在$d$的一个分解$d=(-d_1)(-d_2)$，使$-d_1$与$-d_2$均为负的基本判别式，并有$\chi(\mathfrak{A})=\left(\frac{-d_1}{a}\right)$(Kronecker符号)。那么我们有

$$2^{\frac{1}{2}}\delta_{\mathbb{K}}h_1h_2=w_1w_2\sum_{\mathfrak{A}\in\mathscr{C}_{\mathbb{K}}}\chi(\mathfrak{A})\Psi(\mathfrak{A}),$$

这里$\delta_{\mathbb{K}}=1$或2，视$\mathbb{K}$的基本单位的范是$+1$或-1而定；h_i, w_i $(i=1, 2)$分别为虚二次域$\mathbb{Q}(\sqrt{-d_i})$的类数与单位群的阶；$\Psi(\mathfrak{A})=\Psi\left(\frac{b+\sqrt{d}}{2a}\right)$是在第三章§1.2中定义的Hirzebruch和。

证明　我们的方法与D.Zagier[113]的原来的方法完全不同。

首先，不妨设d_1是一个正奇数。由第三章§2.4的引理2.2，我们有

$$\begin{aligned}&\frac{j}{2}\lim_{s\to1}(\tilde{L}(s,\chi|\mathfrak{A})-\chi(-1)\tilde{L}(s,\chi|\mathfrak{A}^*))\\&=-\frac{\pi}{4\sqrt{d}}\left(\frac{\pi}{2}-\varphi_{\mathfrak{A},j}\right)\frac{\varphi(d_1)}{d_1}\chi(a)\\&\quad+\frac{\pi}{2\sqrt{d}}\chi(a)\sum_{1<m|d_1}\frac{\mu(m)}{m}\left(\mathrm{Im}\log\eta\left(\frac{z_{\mathfrak{A},j}+\frac{1-2aa_1}{2a}b}{m}\right)\right.\\&\quad\left.+\mathrm{Im}\log\eta\left(\frac{z_{\mathfrak{A},j}-\frac{1-2aa_1}{2a}b}{m}\right)\right),\end{aligned}\tag{6.8}$$

这里$\mathfrak{A}^*=\sqrt{d}\mathfrak{A}$；$\tilde{L}(s,\chi|\mathfrak{A})$与$\tilde{L}(s,x|\mathfrak{A}^*)$的定义见第三章§2.2；$j$是一个正整数；$a_1\in\mathbb{Z}$使$2aa_1\equiv1(\mathrm{mod}\ d_1)$；$\varphi$与$\mu$分别是Euler函数与μöbius函数；$\eta$是Dedekind η-函数；

$$z_{\mathfrak{A},j}=\frac{\sqrt{d}}{2a}\left(\frac{\varepsilon_+^j+i\varepsilon_+^{-j}}{|\varepsilon_+^j+i\varepsilon_+^{-j}|}\right)^2,\ \varphi_{\mathfrak{A},j}=\arg z_{\mathfrak{A},j},\ 0<\varphi_{\mathfrak{A},j}<\frac{\pi}{2};$$

ε_+是$\mathbb{K}$的全正基本单位。注意这里我们混用了Dirichlet特征χ与genus特征χ的符号，由genus理论可知这是无妨的。

我们取j使Pell方程

$$x^2-d_1^2dy^2=4,\ x,\ y\in\mathbf{Z}$$

的基本解为

$$\varepsilon_+^j=\frac{U+Vd_1\sqrt{d}}{2}.$$

由此可知有

$$\varphi_{2l,j}=\arcsin\frac{4}{U^2+V^2d_1^2d}. \tag{6.9}$$

根据我们即将在本证明之后加以证明的引理 3.1, 可有

$$\operatorname{Im}\log\eta\left(\frac{z_{2l,j}+\dfrac{b_1}{2a}}{m}\right)+\operatorname{Im}\log\eta\left(\frac{z_{2l,j}-\dfrac{b_1}{2a}}{m}\right)$$
$$=\frac{\pi}{12}(\Phi(M_+)+\Phi(M_-))-\arcsin\frac{U}{\sqrt{U^2+V^2d_1^2d}}, \tag{6.10}$$

这里 $b_1=b(1-2aa_1)$,

$$M_{\pm}=\begin{pmatrix}\dfrac{U\pm b_1d_1V}{2} & -\dfrac{c_1d_1V}{m}\\ ad_1Vm & \dfrac{U\mp b_1d_1V}{2}\end{pmatrix}\in SL_2(\mathbb{Z}),$$

其中 $c_1=\dfrac{b_1^2-d}{4a}\in\mathbb{Z}$。$\Phi(M_\pm)$ 的定义和计算公式见第三章§1。由该处的定理 1.2, 有

$$\Phi(M_\pm)=3+m_0\Psi\left(\frac{\pm b_1+\sqrt{d}}{2am}\right),$$

这里 $\Psi(*)$ 是所谓的 Hirzebruch 和; 正整数 m_0 如下决定之: 首先易见 $g.c.d.(am^2,\ b_1m,\ c_1)$ 是 m 的因子 (实际上由 $g.c.d.(a,\ b_1,\ c_1)=1$, 可知 $g.c.d.(am^2,\ b_1m,\ c_1)=g.c.d.(m,\ c_1)$), 令 η 为 Pell 方程

$$X^2-\left(\frac{m}{g.c.d.(am^2,\ b_1m_1,\ c_1)}\right)^2dY^2=4,\ X,\ Y\in\mathbf{Z}$$

的基本解(即最小解), 则正整数 m_0 使 $\eta^{m_0}=\varepsilon_+^j$。

由 $d_1\mid b_1$, 可得 $d_1\mid c_1$(注意 d_1 奇, 且 $g.c.d.(d_1,\ a)=1$), 于是有 $g.c.d.(am^2,\ b_1m,\ c_1)=g.c.d.(m,\ c_1)=m$。因此 $\eta=\varepsilon_+$, 故 $m_0=j$。即有

$$\Phi(M_\pm) = 3 + j\Psi\left(\frac{\pm b_1 + \sqrt{d}}{2am}\right). \tag{6.11}$$

命

$$\varphi = \arcsin\frac{4}{U^2 + V^2 d_1^2 d}, \quad \psi = \arcsin\frac{V}{\sqrt{U^2 + V^2 d_1^2 d}},$$
$$0 < \varphi, \ \psi < \frac{\pi}{2}, \tag{6.12}$$

则容易算出

$$\cos\left(\frac{\pi}{2} + \varphi\right) = \cos 2\psi = -\frac{-4}{U^2 + V^2 d_1^2 d},$$

故有

$$\frac{\pi}{2} + \varphi = 2\psi. \tag{6.13}$$

计及 $\chi(-1) = -1$，由(6.8)—(6.13)可得

$$\lim_{s\to 1}(\widetilde{L}(s, \chi | \mathbb{A}) + \widetilde{L}(s, \chi | \mathbb{A}^*))$$
$$= \frac{\pi^2}{12\sqrt{d}} \chi(a) \sum_{1 < m | d_1} \frac{\mu(m)}{m}\left(\Psi\left(\frac{b_1 + \sqrt{d}}{2am}\right)\right.$$
$$\left.+ \Psi\left(\frac{-b_1 + \sqrt{d}}{2am}\right)\right), \tag{6.14}$$

这里 $\mathbb{A}$ 为 $\mathfrak{A}$ 所属的类，$\mathbb{A}^*$ 为 $\sqrt{d}\,\mathfrak{A} = \mathfrak{A}^*$ 所属的类。

用 $\chi(\mathbb{A}) = \chi(a)$、$\Psi\left(\frac{-x + \sqrt{d}}{y}\right) = \Psi\left(\frac{x + \sqrt{d}}{y}\right)$（化到约化的，再用第一章的引理 1.5 即得）和第三章的定义 (3.117)，于 (6.14) 中对 $\mathbb{A} \in \mathscr{C}_{\mathbf{K}}$ 求和，即得

$$\delta_{\mathbf{K}} \widetilde{L}(1, \chi) = \frac{\pi^2}{6\sqrt{d}} \sum_{\mathbb{A} \in \mathscr{C}_{\mathbf{K}}} \chi(\mathbb{A}) \sum_{1 < m | d_1} \frac{\mu(m)}{m} \Psi\left(\frac{b_1 + \sqrt{d}}{2am}\right). \tag{6.15}$$

由于

$$\left(\left(am, \ b_1, \ \frac{c_1}{m}\right)\right)$$

是一个判别式 $= b_1^2 - 4ac_1 = d$ 的二元二次原型，所以它一定广义相似于某一个二元二次原型 $((a', b', c'))$，后者判别式当然也是 $d = b'^2 - 4a'c'$，并且对应于理想 $\mathfrak{A}' = \left[a', \frac{-b' + \sqrt{d}}{2}\right]$，这里理

想 $\mathfrak{A}'$ 是定理中开头所说的 $\mathscr{C}_K$ 的某个理想类 A' 的代表理想，满足 $a'>0$ 与 $g.c.d.(a', d)=1$，这样由定义可知，存在 $r, u, s, t\in\mathbb{Z}$，满足 $ru-st=1$，并有 $\delta=\pm1$ 使

$$\delta am = a'r^2+b'rt+c't^2,$$

$$b_1 = 2a'rs+b'(ru+st)+2c'tu,$$

$$\delta\frac{c_1}{m} = a's^2+b'su+c'u^2.$$

令

$$M=\begin{pmatrix} u & s \\ t & r \end{pmatrix}\in SL_2(\mathbb{Z}),$$

并且容易算出

$$M<\frac{b'+\sqrt{d}}{2a'}>=\delta\frac{b_1+\sqrt{d}}{2am}\left(M\langle\xi\rangle\overset{\text{def}}{=}\frac{u\xi+s}{t\xi+r}\right),$$

所以有

$$\Psi\left(\frac{b'+\sqrt{d}}{2a'}\right)=\Psi\left(\delta\frac{b_1+\sqrt{d}}{2am}\right)=\delta\Psi\left(\frac{b_1+\sqrt{d}}{2am}\right). \tag{6.16}$$

又有

$$4a'am\delta=(2a'r+b't)^2-dt^2,$$

因此易得：Kronecker 符号 $\left(\frac{-d_2}{a'am^\delta}\right)=1$，于是

$$\delta=\left(\frac{-d_2}{a}\right)\left(\frac{-d_2}{a'}\right)\left(\frac{-d_2}{m}\right)=\chi(A)\chi(A')\left(\frac{-d_2}{m}\right), \tag{6.17}$$

这里 $\left(\frac{-d_2}{*}\right)$ 均为 Kronecker 符号，其中还用到 $\left(\frac{-d_2}{a}\right)=\left(\frac{-d_1}{a}\right)=\chi(A)$，$\left(\frac{-d_2}{a'}\right)=\left(\frac{-d_1}{a'}\right)=\chi(A')$，这是因为 $\left(\frac{-d_2}{a}\right)\left(\frac{-d_1}{a}\right)=\left(\frac{d}{a}\right)=1$，$\left(\frac{-d_2}{a'}\right)\left(\frac{-d_1}{a'}\right)=\left(\frac{d}{a'}\right)=1$，其中的 $\left(\frac{*}{a}\right)$，$\left(\frac{*}{a'}\right)$ 均为 Kronecker 符号。

我们再来证明由两个不同理想类 A 与 A' 所得出的二次型 $\left(\left(am,\ b_1,\ \frac{c_1}{m}\right)\right)$ 与 $\left(\left(a'm,\ b_1',\ \frac{c_1'}{m}\right)\right)$ 是不可能广义相似的。否

则，由定义就存在 $r, u, s, t\in\mathbb{Z}$，$ru-st=1$，并有 $\delta_1=\pm1$ 使

$$am\delta_1=a'mr^2+b_1'rt+\frac{c_1'}{m}t^2,$$

$$b_1=2a'mrs+b_1'(ru+st)+2\frac{c_1'}{m}tu,$$

$$\frac{c_1}{m}\delta_1=a'ms^2+b_1'su+\frac{c_1'}{m}u^2.$$

由 $d_1\mid b_1'$，$g.c.d.\left(m, \frac{c_1'}{m}\right)=1$，即有 $m\mid t$，故存在 $t_1\in\mathbb{Z}$ 使 $t=mt_1$。令 $s_1=ms\in\mathbb{Z}$，则有 $ru-s_1t_1=1$ 及

$$a\delta_1=a'r^2+b_1'rt_1+c_1't_1^2,$$
$$b_1=2a'rs_1+b_1'(ru+s_1t_1)+2c_1't_1u,$$
$$c_1\delta_1=a's_1^2+b_1's_1u+c_1'u^2,$$

由此即知 $((a, b_1, c_1))$ 广义相似于 $((a', b_1', c_1'))$。这说明 $\mathbb{A}$ 与 $\mathbb{A}'$ 是同一个理想类，这不可能。

由最后这一段的讨论，并用 (6.15)—(6.17)，即得

$$\delta_K\widetilde{L}(1, \chi)=\frac{\pi^2}{6\sqrt{d}}\sum_{\mathbb{A}\in\mathscr{P}_K}\chi(\mathbb{A})\Psi(\mathbb{A})\sum_{1\le m\mid d_1}\frac{\mu(m)}{m}\left(\frac{-d_2}{m}\right),$$

这里及以下 $\left(\frac{-d_2}{*}\right)$ 是 Kronecker 符号。由此可得

$$\delta_K\widetilde{L}(1, \chi)=\frac{\pi^2}{6\sqrt{d}}\prod_{p\mid d_1}\left(1-\frac{1}{p}\left(\frac{-d_2}{p}\right)\right)\sum_{\mathbb{A}\in\mathscr{P}_K}\chi(\mathbb{A})\Psi(\mathbb{A}),\tag{6.18}$$

这里 p 表有理素数。

再由第三章定理 2.3 有

$$\widetilde{L}(1, \chi)=L(1, \chi)L(1, \chi\chi_d),\tag{6.19}$$

这里 $\chi_d(*)=\left(\frac{d}{*}\right)$ 为 Kronecker 符号。由类数公式有

$$L(1, \chi)=\frac{2\pi h_1}{w_1\sqrt{d_1}},\tag{6.20}$$

$$L(1, \chi\chi_d)=L\left(1, \left(\frac{-d_1}{*}\right)\left(\frac{d}{*}\right)\right)$$

$$=L\left(1,\ \left(\frac{-d_2}{*}\right)\right)\prod_{p|d_1}\left(1-\left(\frac{-d_2}{p}\right)\frac{1}{p}\right)$$

$$=\frac{2\pi h_2}{w_2\sqrt{d_2}}\prod_{p|d_1}\left(1-\frac{1}{p}\left(\frac{-d_2}{p}\right)\right),\tag{6.21}$$

这里$\left(\frac{-d_1}{*}\right)$、$\left(\frac{-d_2}{*}\right)$、$\left(\frac{d}{*}\right)$均为 Kronecker 符号。

由(6.18)—(6.21)即得定理的结论。

上面的证明中用到了下述的引理 3.1。我们先介绍一些符号，然后可以自然地得到引理 3.1。

现设 $d>1$, $-k<-1$ 均为基本判别式, m, n, $u\in\mathbb{Z}$, 当 $8|k$ 时, m 也可能是半整数, 即 $2m\in\mathbb{Z}$。再设 n, $u\geqslant 1$ 且 $nu|k$。

设 Pell 方程

$$X^2-k^2dY^2=4,\ X,\ Y\in\mathbb{Z}$$

的基本解(即最小解)为

$$\xi=\frac{U+Vk\sqrt{d}}{2}=\varepsilon_+^j,\tag{6.22}$$

这里 j 为一个正整数, ε_+ 是实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的全正基本单位, 也即 Pell 方程

$$x^2-dy^2=4,\ x,\ y\in\mathbb{Z}$$

的基本解(即最小解): $\varepsilon_+=\frac{t+U\sqrt{d}}{2}$。于是对正整数 a,

$$z_{\mathfrak{A},\xi}\overset{\text{def}}{=\!=}\frac{\sqrt{d}}{2\mathfrak{A}}\left(\frac{\xi+i\xi'}{|\xi+i\xi'|}\right)^2=\frac{2UVkd+4\sqrt{d}i}{2a(U^2+dk^2V^2)}\in\mathbb{H}\tag{6.23}$$

这里 $\mathfrak{A}=\left[a,\ \frac{-b+\sqrt{d}}{2}\right]$是 $\mathbb{K}$ 的一个理想, $c=\frac{-d+b^2}{4a}\in\mathbb{Z}$; $\mathbb{H}$ 是上半平面。

命

$$A=\frac{U\pm bkV}{2},\ B=-ckV,\ C=akV,\ D=\frac{U\mp bkV}{2}.\tag{6.24}$$

易见

$$M=\begin{pmatrix}A & B\\ C & D\end{pmatrix}\in Sl_2(\mathbb{Z}).$$

命

$$z=\frac{\pm b+i\sqrt{d}}{2a}\in\mathbb{H}. \tag{6.25}$$

容易算出

$$M\langle z\rangle\overset{\text{def}}{=\!=}\frac{Az+B}{Cz+D}=z_{\mathfrak{A},j}\pm\frac{b}{2a}, \tag{6.26}$$

由(6.26)可得

$$M_{\pm m}\langle z\pm m\rangle=\pm m\pm\frac{b}{2a}+z_{\mathfrak{A},j}, \tag{6.27}$$

这里

$$M_{\pm m}=\begin{pmatrix}A\pm mC & -(am^2+bm+c)kV\\ C & D\mp mC\end{pmatrix}\in SL_2(\mathbb{Z}). \tag{6.28}$$

由(6.26)与(6.27)不难算得，对 $nu|k$，有

$$M_{\pm m,\frac{u}{n}}\left\langle\frac{u}{n}\left(\pm m\pm\frac{b}{2a}+\frac{i\sqrt{d}}{2a}\right)\right\rangle=\frac{u}{n}\left(\pm m\pm\frac{b}{2a}\pm z_{\mathfrak{A},j}\right), \tag{6.29}$$

其中

$$M_{\pm m,\frac{u}{n}}=\begin{pmatrix}A\pm mC & -(am^2+bm+c)Vk\dfrac{u}{n}\\ aVk\dfrac{n}{u} & D\mp mC\end{pmatrix}\in Sl_2(\mathbb{Z}). \tag{6.30}$$

这样由(6.29)与(6.30)以及第三章的Dedekind η 函数的变换公式(3.18)，有(注意已设 a 为正整数)

$$\begin{aligned}&\log\eta\left(\frac{u}{n}\left(\pm m\pm\frac{b}{2a}+z_{\mathfrak{A},j}\right)\right)\\&=\log\eta\left(M_{\pm m,\frac{u}{n}}\left\langle\frac{u}{n}\left(\pm m\pm\frac{b}{2a}+\frac{i\sqrt{d}}{2a}\right)\right\rangle\right)\\&=\log\eta\left(\frac{u}{n}\left(\frac{i\sqrt{d}}{2a}\pm\frac{b}{2a}\pm m\right)\right)+\frac{\pi i}{12}\Phi(M_{\pm m,\frac{u}{n}})\\&\quad+\frac{1}{2}\log\left(\frac{Vk\sqrt{d}}{2}-\frac{U}{2}i\right),\end{aligned}$$

由此即知有

引理 8.1 在上述记号下，有

$$\mathrm{Im}\log\eta\left(\frac{u}{n}\left(z_{\mathfrak{A},j}+\frac{b}{2a}+m\right)\right)+\mathrm{Im}\log\eta\left(\frac{u}{n}\left(z_{\mathfrak{A},j}-\frac{b}{2a}-m\right)\right)$$

$$=\frac{\pi}{12}\left(\Phi\left(M_{m,\frac{u}{n}}\right)+\Phi\left(M_{-m,\frac{u}{n}}\right)\right)-\arcsin\frac{U}{\sqrt{U^2+dk^2V^2}},$$

这里 a, $b\in\mathbb{Z}$, $a\geqslant1$; $\mathfrak{A}=\left[a,\ \dfrac{-b+\sqrt{d}}{2}\right]$; n, $u\in\mathbb{Z}$, n, $u\geqslant1$, $nu|k$; $d>1$, $-k<-1$ 均为基本判别式; $m\in\mathbb{Z}$, 但在 $8|k$ 时, 也可能 $2m\in\mathbb{Z}$; 其他定义见(6.22)—(6.30)。

3.2 更多的类数公式

在本小节中，我们叙述下列的三个类数公式，即定理3.2—3.4，它们的证明将在§3.3—§3.5中给出。

定理3.2 设 $d>1$ 与 $-k<-1$ 均为基本判别式, $g.c.d.(2d, k)=1$。那么有

$$24\delta_d Jh(-k)h(-dk)=w_{-k}w_{-kd}\sum_{\left\{\mathfrak{A}=\left[a,\frac{-b+\sqrt{d}}{2}\right]\right\}}\sum_{\substack{nu=k\\ n,u\geqslant1}}\chi_u(a)\cdot$$

$$\sum_{m(\bmod a)}\chi_n(am^2+bm+c)\Psi\left(\frac{u}{n}\left(m+\frac{b+\sqrt{d}}{2a}\right)\right),$$

这里 J 是一个正整数, 它使 Pell 方程 $x^2-dk^2y^2=4(x, y\in\mathbb{Z})$ 的最小解为 ε_+^J, 其中 ε_+ 为实二次域 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 的全正基本单位; $h(x)$ 表示域 $\mathbb{Q}(\sqrt{x})$ 的类数; 理想 $\mathfrak{A}=\left[a,\ \dfrac{-b+\sqrt{d}}{2}\right)$ 跑过 $\mathbb{K}$ 的理想类群 $\mathscr{C}_{\mathbb{K}}$ 的一个完全代表元组, 其中 a, b, $c\in\mathbb{Z}$ 满足 $d=b^2-4ac$, $g.c.d.(a, b, c)=1$, $a>0$;

$$\delta_d=\begin{cases}1, & \text{如 } N(\varepsilon)=1, \text{ 即 } \varepsilon_+=\varepsilon;\\ 2, & \text{如 } N(\varepsilon)=-1, \text{ 即 } \varepsilon_+=\varepsilon^2,\end{cases}$$

这里 ε 是 $\mathbb{K}$ 的基本单位; χ_u 与 χ_n 分别为 mod u 与 mod n 的实原特征; 对一个负的基本判别式 $-D$, $w_{-D}=2$, 4, 6, 视 $D>4$, $D=4$, $D=3$ 而定。

定理3.3 设 $d>1$ 与 $-k<-1$ 均为基本判别式, 且 $4\|k$, 以及 $g.c.d.(k, d)=1$。那么有

$$24\delta_d J h(-h)h(-kd)=w_{-k}w_{-kd}\sum_{\{\mathfrak{A}=[a,\frac{-b+\sqrt{d}}{2}]\}}\Bigg(\sum_{\substack{4nu=k\\n,u\geqslant 1}}\chi_u(a)\cdot$$

$$\sum_{m(\bmod 4n)}\chi_{4n}(am^2+bm+c)\Psi\left(\frac{u}{4n}\left(m+\frac{b+\sqrt{d}}{2a}\right)\right)$$

$$+\sum_{\substack{4nu=k\\n,u\geqslant 1}}\chi_{4u}(a)\sum_{m(\bmod n)}\chi_n(am^2+bm+c)$$

$$\left(\eta\Psi\left(\frac{u}{n}\left(m+\frac{b+\sqrt{d}}{2a}\right)\right)-3\Psi\left(\frac{2u}{n}\left(m+\frac{b+\sqrt{d}}{2a}\right)\right)\right.$$

$$\left.+2\Psi\left(\frac{4u}{n}\left(m+\frac{b+\sqrt{d}}{2a}\right)\right)\right)\Bigg),$$

这里的记号与定理 3.2 的相同，而

$$\eta=\begin{cases}1, & \text{如 } d\equiv 1(\bmod 8);\\ 1\text{ 或 }3, & \text{如 } d\equiv 5(\bmod 8),\end{cases}$$

事实上 $\eta=\frac{J}{J'}$，其中正整数 J 与 J' 分别使 ε_+^J 与 $\varepsilon_+^{J'}$ 是 Pell 方程

$$x^2-dk^2y^2=4(x,\ y\in\mathbb{Z})\text{ 与 }X^2-d\left(\frac{k}{4}\right)^2Y^2=4(X,\ Y\in\mathbb{Z})$$

的最小解。

定理 3.4 设 $d>1$ 与 $-k<-1$ 均为基本判别式，且 $8\|k$，$g.c.d.(k,\ d)=1$。那么有

$$24\delta_d J h(-d)h(-kd)=w_{-k}w_{-kd}\sum_{\{\mathfrak{A}=[a,\frac{-b+\sqrt{d}}{2}]\}}\Bigg[\sum_{\substack{8nu=k\\n,u\geqslant 1}}\chi_u(a)$$

$$\cdot\sum_{m(\bmod 8n)}\chi_{8n}(am^2+bm+c)\Psi\left(\frac{u}{8n}\left(m+\frac{b+\sqrt{d}}{2a}\right)\right)$$

$$+\frac{1}{2}\sum_{\substack{8nu=k\\n,u\geqslant 1}}\chi_u(a)\sum_{m(\bmod 8n)}\chi_{8n}(am^2+2bm+4c)$$

$$\Psi\left(\frac{u}{2n}\left(\frac{m}{2}+\frac{b+\sqrt{d}}{2a}\right)\right)$$

$$+\sum_{\substack{8nu=k\\n,u\geqslant 1}}\chi_{8u}(a)\sum_{m(\bmod n)}\chi_n(am^2+bm+c)$$

$$\cdot\left(\Psi\left(\frac{2u}{n}\left(m+\frac{b+\sqrt{d}}{2a}\right)\right)-3\Psi\left(\frac{4u}{n}\left(m+\frac{b+\sqrt{d}}{2a}\right)\right)\right.$$

$$\left.+2\Psi\left(\frac{8u}{n}\left(m+\frac{b+\sqrt{d}}{2a}\right)\right)\right)\Bigg],$$

这里的记号也与定理 3.2 的相同，并且 χ_u 和 χ_{8n} 以及 χ_{8u} 和 χ_n 的合成均为 mod k 的实原特征 $\chi(*)=\left(\frac{-k}{*}\right)$(Kronecker 符号)。

附注 对这几个定理，我们将在 §3.6 中给出一些例子，以便明了它们的作用。

3.3 定理 3.2 的证明

在第三章 §2.4 的定理 2.4 中，取 $\chi(*)=\left(\frac{-k}{*}\right)$(Kronecker 符号)，再注意在例子中的最初说明，即可得

$$\begin{aligned}
&\frac{j}{2}\lim_{s\to1}(\widetilde{L}(s,\chi|\mathfrak{A})+\widetilde{L}(s,\chi|\mathfrak{A}(*)))\\
&=\frac{\pi^2}{12\sqrt{d}}\chi(a)\prod_{p|c}(1-p^{-2})\operatorname{Re}z_{\mathfrak{A},j}\\
&\quad-\frac{\pi}{k\sqrt{d}}\operatorname{Im}\sum_{u=1}^{\infty}e^{2\pi iuz_{\mathfrak{A},j}/c}\sum_{1\leqslant n|u}n^{-1}\sum_{m(\operatorname{mod}k)}\chi(am^2\\
&\quad+bmn+cn^2)\cos\frac{2\pi u}{k}\left(\frac{b}{2a}+\frac{m}{n}\right),
\end{aligned}\tag{6.31}$$

这里还用到第二章 §1.6 的定理 1.8，即 $\sum_{m,n(\operatorname{mod}k)}\chi(am^2+bmn+cn^2)=0$。这在 $g.c.d.(d,k)=1$ 的情况下总是成立的。

注意在定理 3.2 的假定下，$k\equiv3(\operatorname{mod}4)$，$k$ 无平方因子。

对 $z\in\boldsymbol{H}$(上半平面)，有(p 表有理素数)

$$\begin{aligned}
\sum\nolimits_z&\overset{\text{def}}{=}\sum_{u=1}^{\infty}e^{-2\pi iuz/k}\sum_{1\leqslant n|u}n^{-1}\sum_{m(\operatorname{mod}k)}\chi(am^2+bmn+cn^2)\\
&\qquad\cos\frac{2\pi u}{k}\left(\frac{b}{2a}+\frac{m}{n}\right)\\
&=\sum_{\substack{u\geqslant1,g.c.d.(u,k)=1\\ v\geqslant1,p|u\Rightarrow p|k}}e^{\pi iuvz/k}\sum_{\substack{1\leqslant n_1|u\\ 1\leqslant n_2|v}}\frac{1}{n_1n_2}\sum_{m(\operatorname{mod}k)}\\
&\qquad\chi(am^2+bmn_1n_2+cn_1^2n_2^2)\cos\frac{2\pi uv}{k}\left(\frac{b}{2a}+\frac{m}{n_1n_2}\right),
\end{aligned}$$

以 n_1m 代替 m，由 $g.c.d.(n_1,k)=1$，即得

$$\sum\nolimits_z=\sum_{\substack{u\geqslant1,g.c.d.(u,k)=1\\ v\geqslant1,p|v\Rightarrow p|k}}\frac{\sigma(u)}{u}e^{2\pi iuvz/k}\sum_{1\leqslant n|v}\frac{1}{n}\sum_{m(\operatorname{mod}k)}$$

$$(am^2+bmn+cn^2)\cos\frac{2\pi uv}{k}\left(\frac{b}{2a}+\frac{m}{n}\right),\tag{6.32}$$

对上式中的 n，令 $\bar{n}=\prod\limits_{p|n}p$，则 $\bar{n}|k$，故 $k=\bar{n}k_1$，k_1 为一个正整数，并且 $g.c.d.(\bar{n},\ k_1)=1$。由特征分解可知，如令 $m=k_1m_1+\bar{n}m_2$，则从(6.32)可得

$$\sum\nolimits_z=\sum_{\substack{u>1,g.c.d.(u,k)=1\\ v>1,p|v\Rightarrow p|k}}\frac{\sigma(u)}{u}e^{2\pi iuvz/k}\sum_{1<n|v}\frac{1}{n}\sum_{m_1(\bmod \bar{n})}$$

$$\chi_{\bar{n}}(ak_1^2m_1^2+bk_1m_1n+cn^2)\cdot\sum_{m_2(\bmod k_1)}$$

$$\chi_{k_1}(a\bar{n}m_2^2+b\bar{n}m_2n+cn^2)\cos\left(\frac{2\pi uvb}{2ak}+\frac{2\pi uvm_1}{n\bar{n}}+\frac{2\pi uvm_2}{nk_1}\right)$$

$$=\sum_{\substack{u>1,g.c.d.(u,k)=1\\ v>1,p|v\Rightarrow p|k}}\frac{\sigma(u)}{u}e^{2\pi iuvz/k}\sum_{1<n|v}\frac{1}{n}\sum_{m_2(\bmod k_1)}$$

$$\chi_{k_1}(a\bar{n}^2m_2^2+b\bar{n}m_2n+cn^2)$$

$$\cdot\chi_{\bar{n}}(a)\sum_{\substack{m_1(\bmod \bar{n})\\ g.c.d.(m_1,\bar{n})=1}}\cos\left(\frac{2\pi uvb}{2ak}+\frac{2\pi uvm_2}{nk_1}+\frac{2\pi uvm_1}{n\bar{n}}\right),$$

$$\tag{6.33}$$

这里 $\chi_{\bar{n}}$，χ_{k_1} 分别是 mod $\bar{n}$，k_1 的实原特征。对 (6.33) 的最内一层和用 Ramanujan 和的公式(见文献[25]p.237.定理271)，可得

$$\sum\nolimits_z=\sum_{\substack{u>1,g.c.d.(u,k)=1\\ v>1,p|v\Rightarrow p|k}}\frac{\sigma(u)}{u}e^{2\pi iuvz/k}$$

$$\cdot\sum_{1<n|v}\frac{\chi_{\bar{n}}(a)}{n}\sum_{1<l|\bar{n},\frac{v}{n}}l\mu\left(\frac{\bar{n}}{l}\right)\sum_{m_2(\bmod k_1)}\chi_{k_1}(a\bar{n}^2m_2^2$$

$$+b\bar{n}m_2+c)\cos\left(\frac{2\pi uvb}{2ak}+\frac{2\pi uvm_2}{k_1}\right),$$

$$\tag{6.34}$$

以上用到 $g.c.d.(n,\ k_1)=1$，并已用 nm_2 代替 m_2。

注意到 $g.c.d.(\bar{n},\ a)>1$ 时，$\chi_{\bar{n}}(a)=0$，而当 $g.c.d.(\bar{n},\ a)=1$ 时，由 $\bar{n}$ 奇，即有

$$\sum_{m_1(\bmod \bar{n})}\chi_{\bar{n}}(ak_1^2m_1^2+bk_1m_1+c)$$

$$=\chi_{\bar{n}}(a)\sum_{m_1(\bmod \bar{n})}\chi_{\bar{n}}(m_1^2-d)=\chi_{\bar{n}}(a)\tilde{\mu}(\bar{n}), \qquad (6.35)$$

这里 $\tilde{\mu}(\bar{n})$ 为积性函数，且对有理素数 p 有

$$\tilde{\mu}(p)=\begin{cases}-1, & \text{如 } p\nmid d;\\ p-1, & \text{如 } p\mid d.\end{cases}$$

这可由华罗庚著《数论导引》第七章 §8 的结果推出。

这样，由(6.34)与(6.35)即有

$$\sum\nolimits_z=\sum_{\substack{u\geqslant 1,g.c.d.(u,k)=1\\ v\geqslant 1,p\mid v\Rightarrow p\mid k}}\frac{\sigma(u)}{u}e^{2\pi iuvz/k}$$

$$\cdot\sum_{\substack{1\leqslant n\mid v\\ g.c.d.(n,a)=1}}\frac{1}{n\tilde{\mu}(\bar{n})}\sum_{1\leqslant l\mid n,\frac{v}{n}}l\mu\left(\frac{\bar{n}}{l}\right)$$

$$\cdot\sum_{m_1(\bmod \bar{n})}\chi_{\bar{n}}(ak_1^2m_1^2+bk_1m_1+c)\sum_{m_2(\bmod k_1)}\chi_{k_1}(a\bar{n}^2m_2^2+b\bar{n}m_2c)$$

$$\cdot\cos\left(\frac{2\pi uvb}{2ak}+\frac{2\pi uvm_2}{k_1}+\frac{2\pi uvm_1}{\bar{n}}\right), \qquad (6.36)$$

注意 $\bar{n}\mid v$，故在 $\cos(*)$ 的自变量中不妨添上 $\frac{2\pi uvm_1}{\bar{n}}$。这样再用特征合成，由(6.36)即得

$$\sum\nolimits_z=\sum_{\substack{u\geqslant 1,g.c.d.(u,k)=1\\ v\geqslant 1,p\mid v\Rightarrow p\mid k}}\psi(v)\frac{\sigma(u)}{u}e^{2\pi iuvz/k}$$

$$\cdot\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi uv}{k}\left(\frac{b}{2a}+m\right), \qquad (6.37)$$

其中

$$\psi(v)=\sum_{\substack{1\leqslant n\mid v\\ g.c.d.(n,a)=1}}\frac{1}{n\tilde{\mu}(\bar{n})}\sum_{1\leqslant l\mid \bar{n},\frac{v}{n}}l\mu\left(\frac{\bar{n}}{l}\right).$$

易见 $\psi(v)$ 为 v 的积性函数。设 p^α 为有理素数 p 的幂，则容易算出

$$\psi(p^\alpha)=\begin{cases}1, & \text{如 } p\mid a;\\ \dfrac{p+1}{p^\alpha}, & \text{如 } p\nmid a, \text{且 } p\nmid d;\\ \dfrac{p^{\alpha+1}-p-1}{(p-1)p^\alpha}, & \text{如 } p\nmid a, \text{但 } p\mid d.\end{cases} \qquad (6.38)$$

对正整数 u，命

$$\frac{\tilde{\sigma}(u)}{u}=\sum_{\substack{u_1,v\geqslant 1,u_1v=u\\ g.c.d.(u_1,\ )=1\\ p|v\Rightarrow p|k}}\psi(v)\frac{\sigma(u_1)}{u_1} \tag{6.39}$$

则 $\tilde{\sigma}(u)$ 是 u 的积性函数，且对一个有理素数幂 p^α，有

$$\tilde{\sigma}(p^\alpha)=\begin{cases}\sigma(p^\alpha),\ \text{如 } p\nmid k;\\ p^\alpha,\ \text{如 } p|k,\ p|a;\\ p+1,\ \text{如 } p|k,\ p\nmid a,\ p\nmid d;\\ \dfrac{p^{\alpha+1}-p-1}{p-1},\ \text{如 } p|k,\ p\nmid a,\ p|d,\end{cases}$$

但已设 $g.c.d.(d,k)=1$，所以最后一种情况不出现。在第二种情况下，即存在有理素数 p，使 $p|k,a,u$ 时，我们来证明

$$\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi u}{k}\left(\frac{b}{2a}+m\right)=0, \tag{6.40}$$

注意此时应有 $p\nmid d$。命 $k=k_1p$，则 $p\nmid k_1$，用特征分解即知(6.40)的左边等于

$$\sum_{m_1(\bmod p)}\chi_p(ak_1^2m_1^2+bk_1m_1+c)\sum_{m_2(\bmod k_1)}\chi_{k_1}(ap^2m_2^2$$
$$+bpm_2+c)\cos\left(\frac{2\pi ub}{2ak}+\frac{2\pi um_1}{p}+\frac{2\pi um_2}{k_1}\right)$$
$$=\sum_{m_2(\bmod k_1)}\chi_{k_1}(ap^2m_2^2+bpm_2+c)\cos\left(\frac{2\pi ub}{2ak}+\frac{2\pi um_2}{k_1}\right)$$
$$\cdot\sum_{m_1(\bmod p)}\chi_p(bk_1m_1+c)=0,$$

这里用到 $p|a,u,\ p\nmid d$，从而 $p\nmid bk_1$。

这样由(6.37)—(6.40)以及上述讨论，可得

$$\sum\nolimits_3=\sum_{u=1}^{\infty}\frac{\tilde{\sigma}(u)}{u}e^{2\pi i uz/k}\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi u}{k}\left(\frac{b}{2a}+m\right), \tag{6.41}$$

这里 $\tilde{\sigma}(u)$ 为 u 的积性函数，且对一个有理素数幂 p^α 有

$$\tilde{\sigma}(p^\alpha)=\begin{cases}\sigma(p^\alpha),\ \text{如 } p\nmid k;\\ p+1,\ \ \text{如 } p|k,\end{cases}$$

其中 $\sigma(*)$ 为 $*$ 的正因子的和。

对正整数 n，命

$$S(n)=\sum_{1<u\mid n}\mu\left(\frac{n}{u}\right)\tilde{\sigma}(u).$$

则 $S(n)$ 为 n 的积性函数，且对素数幂 p^{α} 有

$$S(p^{\alpha})=\begin{cases}p^{\alpha}, & \text{如 } p\nmid k;\\ p, & \text{如 } p\mid k,\ \text{且 } \alpha=1;\\ 0, & \text{如 } p\mid k,\ \text{且 } \alpha\geqslant 2.\end{cases}$$

即得

$$S(n)=nW(n),$$

这里积性函数 $W(n)$ 满足

$$W(n)=\begin{cases}1, & \text{如 } p\mid g.c.d.(k,n)\Rightarrow p\| n;\\ 0, & \text{否则.}\end{cases} \tag{6.42}$$

这样由反转公式有

$$\tilde{\sigma}(u)=\sum_{1<n\mid u}S(n)=\sum_{1<n\mid u}nW(n). \tag{6.43}$$

于是由(6.41)—(6.43)有

$$\begin{aligned}\sum\nolimits_{z}&=\sum_{u=1}^{\infty}\frac{1}{u}e^{2\pi iuz/k}\sum_{1<n\mid u}nW(n)\sum_{m(\bmod k)}\\&\quad\cdot\chi(am^2+bm+c)\cos\frac{2\pi u}{k}\left(\frac{b}{2a}+m\right)\\&=\sum_{u,n=1}^{\infty}\frac{W(n)}{u}e^{2\pi iunz/k}\sum_{m(\bmod k)}\\&\quad\cdot\chi(am^2+bm+c)\cos\frac{2\pi un}{k}\left(\frac{b}{2a}+m\right),\end{aligned} \tag{6.44}$$

在上式中，令 $n=n_1n_2$，其中 $g.c.d.(n_1,\ k)=1$，$p\mid n_2\Rightarrow p\mid k$。由(6.42)知，这里的 n_2 应为无平方因子的（否则 $W(n_2)=0$，不必计算了），于是 $n_2\mid k$，这样由(6.44)可得

$$\begin{aligned}\sum\nolimits_{z}&=\sum_{u=1}^{\infty}\frac{1}{u}\sum_{\substack{1<l\mid k\\ n>1,\,g.c.d.(n,k)=1}}e^{2\pi iunlz/k}\\&\quad\cdot\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi unl}{k}\left(\frac{b}{2a}+m\right)\\&=\sum_{u=1}^{\infty}\frac{1}{u}\sum_{1<l\mid k}\sum_{n=1}^{\infty}\sum_{1<v\mid n,k}\mu(v)e^{2\pi iunlz/k}\cdot\\&\quad\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi unl}{k}\left(\frac{b}{2a}+m\right)\end{aligned}$$

$$= \sum_{\substack{l,v \mid k \\ l,v>1}} \mu(v) \sum_{u,n=1}^{\infty} \frac{1}{u} e^{2\pi i u n v l z/k}$$

$$\cdot \sum_{m \pmod k} \chi(am^2+bm+c) \cos \frac{2\pi u v n l}{k}\left(\frac{b}{2a}+m\right)$$

$$= \sum_{\substack{l,v \mid k \\ l,v>1}} \mu(v) \sum_{n=1}^{\infty} \frac{\sigma(n)}{n} e^{2\pi i n v z/l}$$

$$\cdot \sum_{m \pmod k} \chi(am^2+bm+c) \cos \frac{2\pi n v}{l}\left(\frac{b}{2a}+m\right), \quad (6.45)$$

其中已用 $\frac{k}{l}$ 代替 l, n 代替 un.

命 $g.c.d.(l, v)=u$, $l=ul_1$, $v=uv_1$, 则 $ul_1v_1 \mid k$, 而由(6.45)得到

$$\sum\nolimits_z = \sum_{\substack{ul_1v_1 \mid k \\ u,l_1,v_1>1}} \mu(u)\mu(v_1) \sum_{n=1}^{\infty} \frac{\sigma(n)}{n} e^{2\pi i n v_1 z/l_1}$$

$$\cdot \sum_{m \pmod k} \chi(am^2+bm+c) \cos \frac{2\pi n v_1}{l_1}\left(\frac{b}{2a}+m\right)$$

$$= \sum_{\substack{lv=k \\ l,v>1}} \mu(v) \sum_{n=1}^{\infty} \frac{\sigma(n)}{n} e^{2\pi i n v z/l}$$

$$\cdot \sum_{m \pmod k} \chi(am^2+bm+c) \cos \frac{2\pi n v}{l}\left(\frac{b}{2a}+m\right), \quad (6.46)$$

其中用到, 对 μöbius 函数 μ 有

$$\sum_{u \mid N} \mu(u)=1 \text{ 或 } 0, \text{ 视 } m=1 \text{ 或 } m>1 \text{ 而定.}$$

再用特征分解, 由(6.46)即得

$$\sum\nolimits_z = \sum_{\substack{lv=k \\ l,v>1}} \mu(v) \sum_{n=1}^{\infty} \frac{\sigma(n)}{n} e^{2\pi i n v z/l} \sum_{m_1 \pmod l} \chi_l(av^2m_1^2+bvm_1+c)$$

$$\cdot \sum_{m_2 \pmod v} \chi_v(al^2m_2^2+blm_2+c)$$

$$\cdot \cos\left(\frac{2\pi n v b}{2al}+\frac{2\pi n v^2 m_1}{l}+2\pi n v m_2\right)$$

$$= \sum_{\substack{lv=k \\ l,v>1}} \mu(v) \sum_{n=1}^{\infty} \frac{\sigma(n)}{n} e^{2\pi i n v z/l} \sum_{m_1 \pmod l} \chi_l(am_1^2+bm_1+c)$$

$$\cdot \cos \frac{2\pi n v}{l}\left(\frac{b}{2a}+m_1\right) \sum_{m_2 \pmod v} \chi_v(am_2^2+bm_2+c),$$

由 $g.c.d.(v, d)=1$ 及 v 奇, 用(6.35)即知最内一层和是

$$\mu(v)\chi_v(a),$$

从而得到

$$\sum_z = \sum_{\substack{lv=k\\ l,v>1}} \chi_v(a) \sum_{n=1}^{\infty} \frac{\sigma(n)}{n} e^{2\pi i n v z/l}$$

$$\cdot \sum_{m(\bmod l)} (\chi_l(am^2+bm+c)\cos\frac{2\pi nv}{l}\left(\frac{b}{2a}+m\right)$$

$$= \frac{1}{2}\sum_{\substack{lv=k\\ l,v>1}} \chi_v(a) \sum_{m(\bmod l)} \chi_l(am^2+bm+c)$$

$$\cdot \sum_{n=1}^{\infty} \frac{\sigma(n)}{n} \left(e^{2\pi i n v\left(z+\frac{b}{2a}+m\right)/l} + e^{2\pi i n v\left(z-\frac{b}{2a}-m\right)/l}\right),$$

再用 Dedekind η 函数，即有

$$\sum_z = \frac{\pi i z}{12} \sum_{\substack{lv=k\\ l,v>1}} \frac{v}{l}\chi_v(a) \sum_{m(\bmod l)} \chi_l(am^2+bm+c)$$

$$-\frac{1}{2}\sum_{\substack{lv=k\\ l,v>1}} \chi_v(a) \sum_{m(\bmod l)} \chi_l(am^2+bm+c)$$

$$\cdot\left(\log\eta\left(\frac{v}{l}\left(z+\frac{b}{2a}+m\right)\right)+\log\eta\left(\frac{v}{l}\left(z-\frac{b}{2a}-m\right)\right)\right). \tag{6.47}$$

(6.47) 的第一项等于

$$\frac{\pi i z}{12} \sum_{\substack{lv=k\\ l,v>1}} \frac{v}{l}\chi_v(a)\chi_l(a)\mu(l) = \frac{\pi i z}{12}\chi(a)k\sum_{1<l|k}\frac{\mu(l)}{l^2}$$

$$= \frac{\pi i z}{12}\chi(a)k\prod_{p|k}(1-p^{-2}), \tag{6.48}$$

这样，由 (6.47) 与 (6.48)，我们得到

$$\sum_z = \frac{\pi i z}{12}\chi(a)k\prod_{p|c}(1-p^{-2})$$

$$-\frac{1}{2}\sum_{\substack{nu=k\\ n,u>1}} \chi_u(a) \sum_{m(\bmod n)} x_n(am^2+bm+c)$$

$$\cdot\left[\log\eta\left(\frac{u}{n}\left(z+\frac{b}{2a}+m\right)\right)+\log\eta\left(\frac{u}{n}\left(z-\frac{b}{2a}-m\right)\right)\right]. \tag{6.49}$$

现在，我们在 (6.31) 中取 $j=J$ 使

$$\varepsilon_+^J=\frac{U+kV\sqrt{d}}{2}$$

为Pell方程

$$x^2-dk^2y^2=4,\ x,\ y\in\mathbb{Z}$$

的基本解(即最小解)。则由(6.49)及引理3.1可知有

$$\begin{aligned}\operatorname{Im}\sum z_{\mathfrak{A},j}=&\frac{\pi\chi(a)k}{12}\prod_{p\mid k}(1-p^{-2})\operatorname{Re}z_{\mathfrak{A},j}-\frac{1}{2}\sum_{\substack{nu=k\\ n,u>1}}\chi_u(a)\\ &\cdot\sum_{m(\bmod n)}\chi_n(am^2+bm+c)\Big[-\arcsin\frac{U}{\sqrt{U^2+dk^2V^2}}\\ &+\frac{\pi}{12}\big(\Phi(M_{m,\frac{u}{n}})+\Phi(M_{-m,\frac{u}{n}})\big)\Big],\end{aligned}\tag{6.50}$$

这里$M_{\pm m,\frac{u}{n}}$如(6.28)所示。

由于当$k=nu$, $g.c.d.(a,\ u)=g.c.d.(am^2+bm+c,\ n)=1$时,有

$$\begin{aligned}&g.c.d.\Big((2am+b)kV,\ (am^2+bm+c)kV\frac{u}{n},\ aVk\frac{n}{u}\Big)\\ &=Vg.c.d.((2am+b)nu,\ (am^2+bm+c)u^2,\ an^2)\\ &=Vg.c.d.(a,\ b,\ c)=V,\end{aligned}$$

故此时由第三章§1.2的定理1.2,即得

$$\begin{aligned}\Phi(M_{\pm m,\frac{u}{n}})&=3+\Psi\left(\frac{\pm(2am+b)kV+\sqrt{U^2-4}}{2aVk\frac{n}{u}}\right)\\ &=3+\Psi\left(\frac{u}{n}\Big(m+\frac{b+\sqrt{d}}{2a}\Big)\right).\end{aligned}\tag{6.51}$$

又

$$\begin{aligned}\sum_{\substack{nu=k\\ n,u>1}}\chi_u(a)\sum_{m(\bmod n)}\chi_n(am^2+bm+c)&=\sum_{\substack{nu=k\\ n,u>1}}\chi_u(a)\mu(n)\chi_n(a)\\ &=\chi_k(a)\sum_{1<n\mid k}\mu(n)=0,\end{aligned}\tag{6.52}$$

这样由(6.31)以及(6.50)—(6.52)可得

$$\begin{aligned}&\frac{J}{2}\lim_{s\to1}(\widetilde{L}(s,\ \chi\mid\mathfrak{A})+\widetilde{L}(s,\ \chi\mid\mathfrak{A}^{(*)}))\\ &=\frac{\pi^2}{12k\sqrt{d}}\sum_{\substack{nu=k\\ n,u>1}}\chi_u(a)\sum_{m(\bmod n)}\chi_n(am^2+bm+c)\end{aligned}$$

$$\cdot \Psi\left(\frac{u}{n}\left(m+\frac{b+\sqrt{d}}{2a}\right)\right), \tag{6.53}$$

令 $\mathfrak{A}$ 跑过 $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ 理想类群 $\mathscr{C}_{\mathbb{K}}$ 的一个完全代表元组，则由第三章的定义(3.117)及定理 2.3，用一下(6.53) 即得定理 3.2。当然还要用一下类数公式而有

$$\tilde{L}(1,\ \chi)=L(1,\ \chi)L(1,\ \chi\chi_d)=\frac{4\pi^2 h(-k)h(-kd)}{w_{-k}w_{-kd}k\sqrt{d}},$$

(6.53)的左边对 $\mathfrak{A}$ 求和是 $\tilde{L}(1,\ \chi)$ 乘以 $\frac{J}{2}\delta_{\mathbb{K}}$。定理 3.2 得证。

3.4 定理 3.3 的证明

本小节中假定 $k=4k_1$，k_1 为无平方因子正整数，$k_1\equiv 1 \pmod 4$，这等价于 $-k<-1$ 为负的基本判别式且 $-k\equiv 12 \pmod{16}$，再设 $g.c.d.(k,\ d)=1$。其他符号如定理 3.3 所述。

对 $z\in\mathbb{H}$，仍记

$$\sum\nolimits_z \stackrel{\text{def}}{=\!=} \sum_{u=1}^{\infty} e^{2\pi i u z/k} \sum_{1<n|u} \frac{1}{n} \sum_{m(\text{mod } k)} \chi(am^2+bmn+cn^2)$$

$$\cdot \cos\frac{2\pi u}{k}\left(\frac{b}{2a}+\frac{m}{n}\right). \tag{6.54}$$

在(6.54)中，命 $u=u_1u_2u_3$，其中 $g.c.d.(u_1,\ k)=1$，u_2 为 2 的幂次，$p|u_3 \Rightarrow p|k_1$，这里与下面的 p 仍表有理素数，则 u，u_3 为正奇数。再命 $n=n_1n_2n_3$，而 $n_l|u_l\ (l=1,2,3)$。最后以 mn_1 代替 m，即可由(6.54)得出

$$\sum\nolimits_z = \sum_{\substack{u_1>1,\, g.c.d.(u_1,k)=1\\ 1<u_2 \text{为2的幂次}\\ u_3>1,\, p|u_3\Rightarrow p|k_1}} e^{2\pi i u_1u_2u_3 z/k} \sum_{\substack{1<n_1|u_1\\ 1<n_2|u_2\\ 1<n_3|u_3}} \frac{1}{n_1n_2n_3}$$

$$\cdot \sum_{m(\text{mod }\ )} \chi(am^2+bmn_2n_3+cn_2^2n_3^2)\cos\frac{2\pi u_1u_2u_3}{k}\left(\frac{b}{2a}+\frac{m}{n_2n_3}\right). \tag{6.55}$$

在(6.55)中，命 $\bar{n}_3=\prod_{p|n_3} p$，则 $k_1=\bar{n}_3k_3$，$\bar{n}_3$，k_3 均为无平方因子正奇数，且 $g.c.d.(k_3,\ n_3)=1$。易见 $k=4\bar{n}_3k_3$。令 $m\mapsto 4\bar{n}_3m_1$

$+k_3\bar{n}_3m_2+4k_3m_3$, 则由(6 55)可得

$$\sum_z=\sum_{\langle u_1,u_2,u_3\rangle}\frac{\sigma(u_1)}{u_1}e^{2\pi iu_1u_2u_3z/k}\sum_{\substack{1\leqslant n_2\mid u_2\\1\leqslant n_3\mid u_3}}\frac{1}{n_2n_3}$$
$$\cdot\sum_{m_1(\bmod k_3)}\chi_{k_3}(16\bar{n}_3^2am_1^2+4\bar{n}_3bm_1n_2n_3+cn_2^2n_3^2)$$
$$\cdot\sum_{m_2(\bmod 4)}\chi_4(ak_3^2\bar{n}_3^2m_2^2+bk_3\bar{n}_3m_2n_2n_3+cn_2^2n_3^2)$$
$$\sum_{m_3(\bmod\bar{n}_3)}\chi_{\bar{n}_3}(16ak_3^2m_3^2+4bk_3m_3n_2n_3+cn_2^2n_3^2)$$
$$\cdot\cos\left(\frac{2\pi u_1u_2u_3b}{2ak}+\frac{2\pi u_1u_2u_3}{kn_2n_3}(4\bar{n}_3m_1+k_3\bar{n}_3m_2+4k_3m_3)\right),\tag{6.56}$$

这里$\langle u_1, u_2, u_3\rangle$表示求和范围与(6.55)的相同，这是为了简写起见，以下也这样表示；上面用到了特征分解，χ_{k_3}, χ_4, $\chi_{\bar{n}_3}$ 分别为 mod k_3, 4, $\bar{n}_3$ 的实原特征。这样可得知(6.56)的最内一层和等于

$$\chi_{\bar{n}_3}(a)\sum_{\substack{m_3(\bmod\bar{n}_3)\\g.c.d.(m_3,\bar{n}_3)=1}}\cos\left(\frac{2\pi u_1u_2u_3b}{2ak}\right.$$
$$\left.+\frac{2\pi u_1u_2u_3}{n_2n_3}\left(\frac{m_1}{k_3}+\frac{m_2}{4}\right)+2\pi\frac{u_2u_3}{n_2n_3}u_1\frac{m_3}{\bar{n}_3}\right)$$
$$=\chi_{\bar{n}_3}(a)\cos\left(\frac{2\pi u_1u_2u_3b}{2ak}+\frac{2\pi u_1u_2u_3}{n_2n_3}\left(\frac{m_1}{k_3}+\frac{m_2}{4}\right)\right)$$
$$\cdot\sum_{1\leqslant l\mid\bar{n}_3,\,u_1\frac{u_2u_3}{n_2n_3}}l\mu\left(\frac{\bar{n}_3}{l}\right),\tag{6.57}$$

这里已用了 Ramanujan 和的公式。注意到 $g.c.d.\left(\bar{n}_3,\ \frac{u_1u_2}{n_2}\right)=1$, 并用 $n_2n_3m_1$ 代替 m_1, n_3m_2 代替 m_2, 则由(6.56)与(6.57)可得

$$\sum_z=\sum_{\langle u_1,u_2,u_3\rangle}\frac{\sigma(u_1)}{u_1}e^{2\pi iu_1u_2u_3z/k}\sum_{1\leqslant n_2\mid u_2}\frac{1}{n_2}\sum_{1\leqslant n_3\mid u_3}\frac{1}{n_3}$$
$$\cdot\sum_{m_1(\bmod k_3)}\chi_{k_3}(16\bar{n}_3^2am_1^2+4\bar{n}_3bm_1+c)$$
$$\cdot\sum_{m_2(\bmod 4)}\chi_4(ak_3^2\bar{n}_3^2m_2^2+bk_3\bar{n}_3m_2n_2+cn_2^2)$$
$$\cdot\cos\left(2\pi u_1u_2u_3\left(\frac{b}{2ak}+\frac{m_1}{k_3}+\frac{m_2}{4n_2}\right)\right)\chi_{\bar{n}_3}(a)\sum_{1\leqslant l\mid\bar{n}_3\cdot\frac{u_3}{n_3}}l\mu\left(\frac{\bar{n}_3}{l}\right)\tag{6.58}$$

与上一小节相同，当 $g.c.d.(\bar{n}_3, a)=1$ 时有

$$\sum_{m_3 (\bmod \bar{n}_3)} \chi_{\bar{n}_3}(16k_3^2 a m_3^2 + 4k_3 b m_3 + c) = \chi_{\bar{n}_3}(a) \tilde{\mu}(\bar{n}_3), \quad (6.59)$$

这里 $\tilde{\mu}$ 的定义与上一小节的相同。

由(6.58)与(6.59)可得

$$\begin{aligned}\sum\nolimits_z = &\sum_{\langle u_1, u_2, u_3 \rangle} \frac{\sigma(u_1)}{u_1} e^{2\pi i u_1 u_2 u_3 z/k} \\ &\cdot \sum_{1 \leqslant n_2 | u_2} \frac{1}{n_2} \sum_{\substack{1 \leqslant n_3 | u_3 \\ g.c.d.(n_3, a)=1}} \frac{1}{n_3 \tilde{\mu}(\bar{n}_3)} \sum_{1 \leqslant l | \bar{n}_3, \frac{u_3}{n_3}} l\mu\left(\frac{\bar{n}_3}{l}\right) \\ &\cdot \sum_{m_1 (\bmod k_1)} \chi_{k_1}(16\bar{n}_3^2 a m_1^2 + 4\bar{n}_3 b m_1 + c) \\ &\cdot \sum_{m_2 (\bmod 4)} \chi_4(a k_3^2 \bar{n}_3^2 m_2^2 + b k_3 \bar{n}_3 m_2 n_2 + c n_2^2) \\ &\cdot \sum_{m_3 (\bmod \bar{n}_3)} \chi_{\bar{n}_3}(16k_3^2 a m_3^2 + 4k_3 b m_3 + c) \\ &\cdot \cos\left(2\pi u_1 u_2 u_3 \left(\frac{b}{2ak} + \frac{m_1}{k_1} + \frac{m_3}{\bar{n}_3} + \frac{m_2}{4n_2}\right)\right),\end{aligned}$$

这里在 $\cos(*)$ 的自变量中可以添上 $2\pi u_1 u_2 u_3 \dfrac{m_3}{\bar{n}_3}$ 是因为 $\bar{n}_3 | u_3$。这样再用特征合成，即可从上式得到

$$\begin{aligned}\sum\nolimits_z = &\sum_{\substack{u \text{正奇数} \\ 1 \leqslant v \text{为2的幂次}}} \frac{\tilde{\sigma}(u)}{u} e^{2\pi i u v z/k} \sum_{1 \leqslant n | v} \frac{1}{n} \\ &\cdot \sum_{m_1 (\bmod k_1)} \chi_{k_1}(16 a m_1^2 + 4 b m_1 + c) \sum_{m_2 (\bmod 4)} \chi_4(a m_2^2 + b m_2 n + c n^2) \\ &\cdot \cos\left(2\pi u v \left(\frac{b}{2ak} + \frac{m_1}{k_1} + \frac{m_2}{4n}\right)\right),\end{aligned} \quad (6.60)$$

这里还用到 $k_3 \bar{n}_3 = k_1 \equiv 1 (\bmod 4)$，而对正奇数 u，有

$$\begin{aligned}\frac{\tilde{\sigma}(u)}{u} = &\sum_{\substack{u_1 u_3 = u \\ u_1 \geqslant 1, g.c.d.(u_1, k)=1 \\ u_3 \geqslant 1, p | u_3 \Rightarrow p | k}} \frac{\sigma(u_1)}{u_1} \sum_{\substack{1 \leqslant n_3 | u_3 \\ g.c.d.(n_3, a)=1}} \frac{1}{n_3 \tilde{\mu}(\bar{n}_3)} \\ &\cdot \sum_{1 \leqslant l | \bar{n}_3, \frac{u_3}{n_3}} l\mu\left(\frac{\bar{n}_3}{l}\right),\end{aligned}$$

易见 $\tilde{\sigma}(u)$ 是 u 的积性函数，且当 u 为奇素数的幂 p^α 时，有

$$\tilde{\sigma}(p^{\alpha})=\begin{cases}\sigma(p^{\alpha}), \text{ 如 } p\nmid k_1;\\ p^{\alpha}, \quad \text{ 如 } p|k_1,\ p|a;\\ p+1, \text{ 如 } p|k_1,\ p\nmid a,\ p\nmid d;\\ \dfrac{p^{\alpha+1}-p-1}{p-1}, \text{ 如 } p|k_1,\ p\nmid a,\ p|d.\end{cases}$$

由于 $g.c.d.(k, d)=1$, 可如上一小节一样证明, 当 $p|a,\ k_1,\ u$ 时,

$$\sum_{m_1(\bmod k_1)}\chi_{k_1}(16am_1^2+4bm_1+c)$$
$$\cos\left(2\pi uv\left(\frac{b}{2ak}+\frac{m_1}{k_1}+\frac{m_2}{4n}\right)\right)=0,$$

注意其中的 n 是 2 的幂次且 $n|v$. 因此不妨对奇素数 p, 命

$$\tilde{\sigma}(p^{\alpha})=\begin{cases}\sigma(p^{\alpha}), \text{ 如 } p\nmid k_1;\\ p+1, \quad \text{ 如 } p|k_1,\end{cases}\tag{6.61}$$

而使(6.60)成立。

下列引理可以直接验证。

引理 3.2 设 $1\leqslant n|u$, 且 n 为 2 的正幂次, 则

$$\sum_{m(\bmod 4)}\chi_4(am^2+bmn+cn^2)\,e^{2\pi i\frac{u}{n}\frac{m}{4}}$$

$$\begin{cases}=0, \text{ 如 } \dfrac{u}{n} \text{ 为奇数};\\ \\ =\chi_4(a)\cdot 2\cdot(-1)^{\frac{n}{2}+\frac{u}{2n}}, \text{ 如 } \dfrac{u}{n} \text{ 为偶数},\end{cases}$$

这里 a, b, c 如定理 3.3 所设。

把(6.60)中的 n 区分为 $n=1$ 和 n 为偶数两种情况, 并用引理 3.2, 可得

$$\sum\nolimits_{s}=\sum_{\substack{u\text{正奇数}\\ 1<v\text{为2的幂次}}}\frac{\tilde{\sigma}(u)}{u}\,e^{2\pi iuvz/k}$$

$$\cdot\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi uv}{k}\left(m+\frac{b}{2a}\right)$$

$$+\chi_4(a)\sum_{\substack{u\text{正奇数}\\ 1<v\text{为2的幂次}}}\frac{\tilde{\sigma}(u)}{u}\psi(v)\,e^{2\pi iuvz/k}$$

$$\sum_{m(\bmod k_1)} \chi_{k_1}(16am^2+4bm+c)\cos\frac{2\pi uv}{k}\left(m+\frac{b}{2a}\right),$$

其中

$$\psi(v)=\sum_{\substack{1\leqslant n\mid v\\ 2\mid n,\frac{v}{n}}}\frac{2}{n}(-1)^{\frac{n}{2}+\frac{v}{2n}}.$$

易见对 $v=2^\alpha(\alpha\geqslant 0)$ 有

$$\psi(2^\alpha)=\begin{cases}0, & \text{如 } 0\leqslant\alpha\leqslant 1;\\ 1, & \text{如 } \alpha=2;\\ -\dfrac{3}{2^{\alpha-2}}, & \text{如 } \alpha\geqslant 3.\end{cases}$$

所以有

$$\sum\nolimits_s = I_1+\chi_4(a)I_2-\frac{3}{2}\chi_4(a)I_3. \tag{6.62}$$

其中

$$I_1=\sum_{\substack{u\text{正奇数}\\ \alpha\geqslant 0}}\frac{\tilde{\sigma}(u)}{u}e^{2\pi i2^\alpha uz/k}$$

$$\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi 2^\alpha u}{k}\left(m+\frac{b}{2a}\right),$$

$$I_2=\sum_{u\text{正奇数}}\frac{\tilde{\sigma}(u)}{u}e^{2\pi iuz/k_1}$$

$$\sum_{m(\bmod k_1)}\chi_{k_1}(16am^2+4bm+c)\cos\frac{2\pi u}{k_1}\left(4m+\frac{b}{2a}\right),$$

$$I_3=\sum_{\substack{u\text{正奇数}\\ \alpha\geqslant 0}}\frac{\tilde{\sigma}(u)}{2^\alpha u}e^{4\pi iu2^\alpha z/k_1}$$

$$\sum_{m(\bmod k_1)}\chi_{k_1}(16am^2+4bm+c)\cos\frac{4\pi 2^\alpha u}{k_1}\left(4m+\frac{b}{2a}\right).$$

以下来计算 I_1, I_2, I_3.

对正奇数 n, 命

$$S(n)=\sum_{1\leqslant u\mid n}\mu\left(\frac{n}{u}\right)\tilde{\sigma}(u), \tag{6.63}$$

则不难由(6.61)证明

$$S(n)=nW(n), \tag{6.64}$$

这里对正奇数 n,

$$W(n)=\begin{cases}1, & \text{如 } p\,|\,g.c.d.(k_1,\ n)\Longrightarrow p\,\|\,n;\\ 0, & \text{否则。}\end{cases}\tag{6.65}$$

这样用反转公式可由上述公式(6.63)—(6.65)得出

$$I_1=\sum_{\substack{u,n\text{正奇数}\\ \alpha>0}}\frac{W(n)}{u}e^{2\pi i2^\alpha unz/k}\cdot\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi2^\alpha un}{k}\left(m+\frac{b}{2a}\right)$$

$$=\sum_{\substack{\alpha>0,u,n\text{正奇数}\\ p|g.c.d.(n,k_1)\to p\|n}}\frac{1}{u}e^{2\pi i2^\alpha uvz/k}\cdot\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi2^\alpha un}{k}\left(m+\frac{b}{2a}\right),$$

我们命 $n=n_1n_2$，其中 $g.c.d.(n_1,\ k_1)=1$，而 $p\,|\,n_2\Longrightarrow p\,|\,k_1$，则 n_2 应为无平方因子，从而 $n_2\,|\,k_1$，因此可得

$$I_1=\sum_{\substack{\alpha>0\\ u\text{正奇数}}}\frac{1}{u}\sum_{\substack{1<l|k_1\\ n\text{正奇数},g.c.d.(n,k_1)=1}}e^{2\pi i2^\alpha unlz/k}\cdot\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi2^\alpha unl}{k}\left(m+\frac{b}{2a}\right)$$

$$=\sum_{\substack{\alpha>0\\ u\text{正奇数}}}\frac{1}{u}\sum_{\substack{1<l|k_1\\ n\text{正奇数}}}\sum_{1<v|n,k_1}\mu(v)e^{2\pi i2^\alpha unz/(4l)}\cdot\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi2^\alpha uv}{4l}\left(\frac{b}{2a}+m\right),$$

以上已用 $\frac{k_1}{l}$ 代替 l。于是

$$I_1=\sum_{\substack{\alpha>0\\ u,n\text{正奇数}}}\frac{1}{u}\sum_{\substack{l,v|k_1\\ l,v>1}}\mu(v)e^{2\pi i2^\alpha unv/(4l)}\cdot\sum_{m(\bmod k)}\chi(am^2+bm+c)\cos\frac{2\pi2^\alpha unv}{4l}\left(\frac{b}{2a}+m\right).\tag{6.66}$$

在(6.66)中命 $l=l_1w$，$v=v_1w$，$g.c.d.(l_1,\ v_1)=1$，则 $l_1v_1w\,|\,k_1$。再命 $m\mapsto 4lm_2+vm_1$，并用特征分解，则由(6.66)可得

$$I_1=\sum_{\substack{\alpha>\\ n\text{正奇数}}}\frac{\sigma(n)}{n}\sum_{\substack{lv=k_1\\ l,v>1}}\chi_v(a)e^{2\pi i2^\alpha nvz/(4l)}.$$

$$\sum_{m(\bmod 4l)} \chi_{4l}(am^2+bm+c)\cos\left(\frac{2\pi 2^{\alpha} nv}{4l}\left(\frac{b}{2a}+m\right)\right), \tag{6.67}$$

这里用了

$$\sum_{m(\bmod v)} \chi_v(16l^2am^2+4lbm+c)=\mu(v)\chi_v(a),$$

这与上一小节的(6.35)是类似的。

不难证明，当 $\alpha\geqslant 1$，而 l, n, v 均奇时，有

$$\begin{aligned}\sum_{m(\bmod 4)} \chi_4(al^2m^2+blm+c)e^{2\pi i 2^{\alpha} nvm/4} &= \chi_4(c)+\chi_4(2bl+c)\\ &+(-1)^{2^{\alpha-1}}(\chi_4(al^2+bl+c)+\chi_4(al^2-bl+c))=0,\end{aligned}$$

注意 b 奇(因 d 奇)。

所以，当 $\alpha\geqslant 1$ 时，(6.67) 的最内一层和等于 0。这样，由 (6.67)可得

$$\begin{aligned}I_1 &= \sum_{\substack{\alpha\geqslant 0\\ n\text{正奇数}}} \frac{\sigma(n)}{n}\cdot\frac{\sigma(2^{\alpha})}{2^{\alpha}} \sum_{\substack{lv=k_1\\ l,v\geqslant 1}} \chi_v(a)e^{2\pi i 2^{\alpha} nvz/(4l)}\\ &\quad\cdot\sum_{m(\bmod 4l)} \chi_{4l}(am^2+bm+c)\cos\frac{2\pi 2^{\alpha} nv}{4l}\left(\frac{b}{2a}+m\right)\\ &= \sum_{\substack{lv=k_1\\ l,v\geqslant 1}} \chi_v(a)\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{2\pi i nvz/(4l)}\\ &\quad\cdot\sum_{m(\bmod 4l)} \chi_{4l}(am^2+bm+c)\cos\frac{2\pi nv}{4l}\left(\frac{b}{2a}+m\right),\end{aligned}$$

再用 Dedekind η 函数，即有

$$\begin{aligned}I_1 &= -\frac{1}{2}\sum_{4nu=k}\chi_u(a)\sum_{m(\bmod 4n)}\chi_{4n}(am^2+bm+c)\\ &\quad\cdot\left(\log\eta\left(\frac{u}{4n}\left(z+\frac{b}{2a}+m\right)\right)+\log\eta\left(\frac{u}{4n}\left(z-\frac{b}{2a}-m\right)\right)\right),\end{aligned} \tag{6.68}$$

这里用到

$$\sum_{4nu=k}\frac{u}{n}\chi_u(a)\sum_{m(\bmod 4n)}\chi_{4n}(am^2+bm+c)=0,$$

这是因为刚才已算过，内和等于 0。

用证明(6.67)的相同方法，可以证明

$$I_2=\sum_{\substack{lv=k_1\\l,v>1}}\chi_v(a)\sum_{n\text{正奇数}}\frac{\sigma(n)}{n}\ e^{2\pi invz/l}$$

$$\cdot\sum_{m(\bmod l)}\chi_l(am^2+bm+c)\cos\frac{2\pi nv}{l}\left(\frac{b}{2a}+m\right),$$

与

$$I_3=\sum_{\substack{lv=k_1\\l,v>1}}\chi_v(a)\sum_{\substack{\alpha>0\\n\text{正奇数}}}\frac{\sigma(n)}{2^\alpha n}\ e^{4\pi i2^\alpha nvz/l}$$

$$\cdot\sum_{m(\bmod l)}\chi_l(am^2+bm+c)\cos\frac{4\pi 2^\alpha nv}{l}\left(\frac{b}{2a}+m\right).$$

容易证明

$$\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}f(n)-3\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}f(2n)+2\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}f(4n)$$

$$=\sum_{n\text{正奇数}}\frac{\sigma(n)}{n}f(n)-\frac{3}{2}\sum_{\substack{\alpha>0\\n\text{正奇数}}}\frac{\sigma(n)}{2^\alpha n}f(2^{\alpha+1}n),$$

只要涉及到的级数是绝对收敛的。

这样，可得

$$\chi_4(a)\left(I_2-\frac{3}{2}I_3\right)=-\frac{1}{2}\sum_{\substack{nu=k_1\\n,u>1}}\chi_{4u}(a)\sum_{m(\bmod n)}\chi_n(am^2+bm+c)$$

$$\cdot\left(\log\eta\left(\frac{u}{n}\left(z+\frac{b}{2a}+m\right)\right)+\log\eta\left(\frac{u}{n}\left(z-\frac{b}{2a}-m\right)\right)\right.$$

$$-3\log\eta\left(\frac{2u}{n}\left(z+\frac{b}{2a}+m\right)\right)-3\log\eta\left(\frac{2u}{n}\left(z-\frac{b}{2a}-m\right)\right)$$

$$\left.+2\log\eta\left(\frac{4u}{n}\left(z+\frac{b}{2a}+m\right)\right)+2\log\eta\left(\frac{4u}{n}\left(z-\frac{b}{2a}-m\right)\right)\right)$$

$$+\frac{\pi i}{12}z\chi(a)k\prod_{p|k}(1-p^{-2}),\tag{6.69}$$

最后一项来源于

$$\frac{1}{2}\sum_{4nu=k}\chi_{4u}(a)\sum_{m(\bmod n)}\chi_n(am^2+bm+c)$$

$$\cdot\frac{\pi i}{12}\left(\frac{u}{n}\left(z+\frac{b}{2a}+m\right)+\frac{u}{n}\left(z-\frac{b}{2a}-m\right)\right)(1-3\times 2+2\times 4)$$

$$=\frac{\pi i}{4}z\sum_{4nu=k}\frac{u}{n}\chi_{4u}(a)\sum_{m(\bmod n)}\chi_n(am^2+bm+c)$$

$$= \frac{\pi \mathrm{i}}{4} z \sum_{4nu=k} \frac{u}{n} \chi_{4u}(a)\chi_n(a)\mu(n) = \frac{\pi \mathrm{i}}{4} z\chi(a)k_1 \sum_{1\leqslant n|k_1} \frac{\mu(n)}{n^2}$$

$$= \frac{\pi \mathrm{i}}{12} z\chi(a)k \prod_{p|k}(1-p^{-2}).$$

这样，把(6.68)与(6.69)代入(6.62)，并用第三章的§2.4定理2.4、定义(3.117)、定理2.3和本节的引理3.1，再取正整数 $j=J$ 使

$$\varepsilon_+^J = \frac{U+\sqrt{d}\,kV}{2}$$

为 Pell 方程

$$X^2 - dk^2Y^2 = 4,\ X,\ Y \in \mathbb{Z}$$

的最小解，其中 ε_+ 为 $K=\mathbb{Q}(\sqrt{d})$ 的全正基本单位，则有

$$\frac{J}{2}\delta_K L(1,\ \chi)L(1,\ \chi\chi_d) = \sum_{\{\mathfrak{A}=[a,\frac{-b+\sqrt{d}}{2}]\}} \Bigg(\frac{\pi}{2k\sqrt{d}} \sum_{\substack{4nu=k\\ n,u\geqslant 1}} \chi_u(a)$$

$$\cdot \sum_{m(\bmod 4n)} \chi_{4n}(am^2+bm+c)\Bigg(-\arcsin\frac{U}{\sqrt{U^2+dk^2V^2}}$$

$$+\frac{\pi}{12}(\Phi(M_{m,\frac{u}{4n}})+\Phi(M_{-m,\frac{u}{4n}}))\Bigg)+$$

$$+\frac{\pi^2}{24k\sqrt{d}} \sum_{\substack{4nu=k\\ n,u\geqslant 1}} \chi_{4u}(a) \sum_{m(\bmod n)} \chi_n(am^2+bm+c)(\Phi(M_{m,\frac{u}{n}})$$

$$+\Phi(M_{-m,\frac{u}{n}})-3\Phi(M_{m,\frac{2u}{n}})-3\Phi(M_{-m,\frac{2u}{n}})$$

$$+2\Phi(M_{m,\frac{4u}{n}})+2\Phi(M_{-m,\frac{4u}{n}}))\Bigg), \tag{6.70}$$

这里，对 $nu|k$，有

$$M_{\pm m,\frac{u}{n}} = \begin{pmatrix} \frac{U\pm bkV}{2} \pm amkV & -(am^2+bm+c)Vk\frac{u}{n} \\ aVk\frac{n}{u} & \frac{U\mp bkV}{2}\mp amkV \end{pmatrix}$$

$$\in SL_2(\mathbb{Z}).$$

由第三章§1.2的定理1.2即知，对 $nu|k$，$g.c.d.(u,\ a)=g.c.d.(am^2+bm+c,\ n)=1$ 有

$$\Phi(M_{\pm m,\frac{u}{n}}) = 3+J\left(\frac{k}{nu}\right)\Psi\left(\frac{u}{n}\cdot\frac{\pm(2am+b)+\sqrt{d}}{2a}\right),$$

这里对 $1\leqslant t|k$，$J(t)=\dfrac{J}{J'}$ 是一个正整数，其中 J' 也是一个正整数，它使 Pell 方程

$$\chi^2-d\left(\frac{k}{t}\right)^2y^2=4,\ x,\ y\in\mathbb{Z}$$

的最小解为 $\varepsilon_+^{J'}$。

在我们的情况下，$\dfrac{k}{un}=1,\ 2,\ 4$，容易看到有

$J(1)=J(2)=1$；$\eta\overset{\text{def}}{=\!=}J(4)=1$，如 $d\equiv1(\bmod 8)$；或 1 或 3，如 $d\equiv5(\bmod 8)$。

已证

$$\sum_{m(\bmod 4n)}\chi_{4n}(am^2+bm+c)=0,\ \text{如}\ n\,|\,k_1,$$

则由(6.70)及类数公式，即可得出定理 3.3。

3.5　定理 3.4 的证明

现设 $-k<-1$ 为负的基本判别式，$8\|k$，$k=8k_1$。命

$$\chi_8(*)=\begin{cases}\left(\dfrac{8}{*}\right),\ \text{如}\ k_1\equiv3(\bmod 4);\\[2ex]\left(\dfrac{-8}{*}\right),\ \text{如}\ k_1\equiv1(\bmod 4),\end{cases}$$

其中$\left(\dfrac{8}{*}\right)$与$\left(\dfrac{-8}{*}\right)$ 均为 Kronecker 符号。再设 $g.c.d.(k,\ d)=1$，其他符号如定理 3.4 所述。

我们首先来证明下面的引理。

引理 3.3　设 $n\geqslant1$ 且为 2 的幂次，u 为有理整数，$n|u$。其他符号见上所述，则有

$$\sum_{m(\bmod 8)}\chi_8(am^2+bmn+cn^2)e^{2\pi i\frac{u}{n}\frac{m}{8}}$$

$$\begin{cases}0,\ \text{如}\ n=1,\ u\ \text{偶};\\ 2\chi_8(a+b+c)e^{\frac{i\pi u}{4}}+2\chi_8(c)+2\chi_8(a-b+c)e^{-\frac{i\pi u}{4}}\\ \quad+2\chi_8(4a+2b+c)e^{\frac{i\pi u}{2}},\end{cases}$$

$$
=\begin{cases} \text{如 } n=1,\ u \text{ 奇;} \\ 0,\ \text{如 } n=2,\ \text{且 } 2\|u \text{ 或 } 8|u; \\ i4\left(\dfrac{-8}{u/4}\right)\chi_8(a+2b+4c),\ \text{如 } n=2,\ \text{且 } 4\|u; \\ 0,\ \text{如 } 4|n,\ \text{且 } 4n\nmid u; \\ (-1)^{\frac{n}{4}+\frac{u}{4n}}\cdot 4\cdot\chi_8(a),\ \text{如 } 4|n,\ \text{且 } 4n|u. \end{cases}
$$

证明 直接计算可得。

与3.3、3.4两小节一样，对 $z\in H$，命

$$
\sum\nolimits_z \overset{\text{def}}{=\!=} \sum_{u=1}^{\infty} e^{2\pi i uz/k} \sum_{1<n|u} n^{-1} \sum_{m(\bmod k)} \chi(am^2+bmn+cn^2) \cdot\cos\frac{2\pi u}{k}\left(\frac{b}{2a}+\frac{m}{n}\right), \tag{6.71}
$$

则可证明

$$
\begin{aligned}
\sum\nolimits_z = & \sum_{\substack{u\text{正奇数}\\ 1<v\text{为 2 的幂次}}} \frac{\tilde{\sigma}(u)}{u}\, e^{2\pi i uvz/k} \\
& \cdot\sum_{1<n|v} n^{-1} \sum_{m_1(\bmod k_1)} \chi_{k_1}(64am_1^2+8bm_1+c) \\
& \cdot\sum_{m(\bmod 8)} \chi_8(ak_1^2m^2+bk_1mn+cn^2) \\
& \cdot\cos\left(2\pi uv\left(\frac{b}{2ak}+\frac{m_1}{k_1}+\frac{m}{8n}\right)\right),
\end{aligned} \tag{6.72}
$$

这里 $\tilde{\sigma}(u)$ 为积性函数，且当 u 为奇素数幂 p^{α} 时，有

$$
\tilde{\sigma}(p^{\alpha}) = \begin{cases} \sigma(p^{\alpha}),\ \text{如 } p\nmid k_1; \\ p+1,\ \text{如 } p|k_1. \end{cases}
$$

(6.72)中的 n 分别对 $n=1,2$ 与被4除尽的情况，用引理3.3，并注意由于 k_1 奇，故可用 ak_1^2，bk_1，c 代替 a，b，c。这样可得

$$
\sum\nolimits_z = I_1+I_2+I_3,
$$

其中

$$
I_1 = \sum_{\substack{u\text{正奇数}\\ \alpha>0}} \frac{\tilde{\sigma}(u)}{u}\, e^{2\pi i 2^{\alpha}uz/k} \cdot\sum_{m(\bmod k)} \chi(am^2+bm+c)\cos\frac{2\pi 2^{\alpha}u}{k}\left(\frac{b}{2a}+m\right),
$$

$$I_2=\frac{1}{2}\sum_{\substack{u\text{正奇数}\\ \alpha>0}}\frac{\tilde{\sigma}(u)}{u}e^{2\pi i 2^{\alpha+1}uz/k}$$
$$\cdot\sum_{m(\bmod k)}\chi(am^2+2bm+4c)\cos\frac{2\pi 2^{\alpha}u}{k}\left(\frac{b}{a}+m\right),$$

以及

$$I_3=\chi_8(a)\sum_{\substack{u\text{正奇数}\\ \alpha>0}}\frac{\tilde{\sigma}(u)}{u}\Phi(2^{\alpha})e^{4\pi i 2^{\alpha}uz/k_1}$$
$$\cdot\sum_{m(\bmod k_1)}\chi_{k_1}(am^2+bm+c)\cos\frac{4\pi 2^{\alpha}u}{k_1}\left(\frac{b}{2a}+m\right),$$

这里

$$\Phi(2^{\alpha})=\begin{cases}1, & \text{如 } \alpha=0;\\ -\dfrac{3}{2^{\alpha}}, & \text{如 } \alpha\geqslant 1.\end{cases}$$

用引理 3.3 以及与 §3.3、§3.4 相同的办法，可以证明

$$I_1=\sum_{\substack{lv=k_1\\ l,v>1}}\chi_v(a)\sum_{m(\bmod 8l)}\chi_{8l}(am^2+bm+c)$$
$$\cdot\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{2\pi i nvz/(8l)}\cos\frac{2\pi nv}{8l}\left(\frac{b}{2a}+m\right),$$

$$I_2=\frac{1}{2}\sum_{\substack{lv=k_1\\ l,v>1}}\chi_v(a)\sum_{m(\bmod 8l)}\chi_{8l}(am^2+2bm+4c)$$
$$\cdot\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{2\pi i nvz/(2l)}\cos\frac{2\pi nv}{4l}\left(\frac{b}{a}+m\right),$$

$$I_3=\sum_{\substack{lv=k_1\\ l,v>1}}\chi_{8v}(a)\sum_{m(\bmod l)}\chi_l(am^2+bm+c)$$
$$\cdot\left(\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{4\pi i nvz/l}\cos\frac{4\pi nv}{l}\left(\frac{b}{2a}+m\right)\right.$$
$$-3\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{8\pi i nvz/l}\cos\frac{8\pi nv}{l}\left(\frac{b}{2a}+m\right)$$
$$\left.+2\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{16\pi i nvz/l}\cos\frac{16\pi nv}{l}\left(\frac{b}{2a}+m\right)\right).$$

这样，用 Dedekind η-函数、引理 3.1、定义(3.117)、第三章的定理 2.3 与定理 2.4 以及类数公式，与 §3.3 和 §3.4 同样可以完成定理 3.5 的证明，我们不再详述有关细节，有兴趣的读者可自行

补出。

定理 3.4 证毕。

3.6 例 子

对上述的定理 3.1—3.5, 我们讨论一些例子。

例 1 (F.Hirzebruch) 设有理素数 $p\equiv 3 \pmod 4$, 且 $p>3$。如果实二次域 $Q(\sqrt{p})$ 的类数为 1, 则由定理 3.1 可知虚二次域 $Q(\sqrt{-p})$ 的类数 $h(-p)$ 满足

$$3h(-p)=\Psi(\sqrt{p}).$$

例 2 设有理素数 $p\equiv 1 \pmod 4$。如实二次域 $Q(\sqrt{p})$ 的类数为 1, 则由定理 3.2 可知虚二次域 $Q(\sqrt{-3p})$ 的类数 $h(-3p)$ 满足

$$4Jh(-3p)=\Psi\left(\frac{1+3\sqrt{p}}{2}\right)-2\xi\Psi\left(\frac{1+\sqrt{p}}{6}\right)+(2\xi-1)\Psi\left(\frac{3+\sqrt{p}}{6}\right),$$

其中 $J=1$, 2 或 3 使 Pell 方程

$$x^2-9py^2=4,\ x,\ y\in \mathbb{Z}$$

的最小解为 ε_+^J, 其中 ε_+ 为实二次域 $Q(\sqrt{p})$ 的全正基本单位; $\xi=\left(\frac{p-1}{3}\right)$(后者是 Legendre 符号)。

特别 $p=5$ 时, $J=2$, $\xi=1$, 以及

$$\Psi\left(\frac{1+3\sqrt{5}}{2}\right)=-\Psi\left(\frac{1+\sqrt{5}}{6}\right)=\Psi\left(\frac{3+\sqrt{5}}{6}\right)=4,$$

与 $h(-15)=2$ 吻合。

例 3 设 q 是一个素数, 且 $q\equiv 3 \pmod 4$。如 $p=2q+1$ 仍为一个素数, 则有

$$6h(-p)h(-2p)=\Psi(p\sqrt{2}),$$

这里 $h(-p)$ 与 $h(-2p)$ 分别为虚二次域 $Q(\sqrt{-p})$ 与 $Q(\sqrt{-2p})$ 的类数。

这是因为在定理 3.2 中取 $k=p\equiv 7 \pmod 8)$, $d=8$, 可有

$$12Jh(-p)h(-8p)=\Psi(p\sqrt{2})+\sum_{m=1}^{p}\left(\frac{m^2-2}{p}\right)\Psi\left(\frac{m+\sqrt{2}}{p}\right), \tag{6.73}$$

这里$\left(\frac{*}{p}\right)$是 Legendre 符号，$J=J(p)$是一个正整数，它使 Pell 方程

$$x^2-8p^2y^2=4,\ x,\ y\in Z$$

的最小解为$(3+2\sqrt{2})^J$。

容易证明$J\mid\frac{1}{2}\left(p-\left(\frac{2}{p}\right)\right)=q$，故$J=q$。判别式为$8p^2$的二元二次原型类群的阶由第二章可知是

$$H(8p^2)=\frac{1}{J}\left(p-\left(\frac{2}{p}\right)\right)=2.$$

这个类群的完全代表元组是$\{x^2-2p^2y^2,\ -x^2+2p^2y^2\}$。由此不难证明

$$\left(\frac{m^2-2}{p}\right)\Psi\left(\frac{m+\sqrt{2}}{p}\right)=\Psi(p\sqrt{2}),\ 如\ p\nmid m^2-2. \tag{6.74}$$

这样由(6.73)与(6.74)即得所需。

例 4 设有理素数$p\equiv1\pmod 8$，则当实二次域$Q(\sqrt{p})$的类数为1时，虚二次域$Q(\sqrt{-p})$的类数$h(-p)$满足

$$3h(-p)=\Psi(\sqrt{4p}).$$

这可在定理3.3中取$k=4$，$d=p$而得到。

例 5 设有理素数$p\equiv5\pmod 8$，则当实二次域$Q(\sqrt{p})$的类数为1时，虚二次域$Q(\sqrt{-p})$的类数$h(-p)$满足

$$3Jh(-p)=\Psi(\sqrt{4p})+\xi\left(\Psi\left(\frac{3+\sqrt{p}}{8}\right)-\Psi\left(\frac{1+\sqrt{p}}{8}\right)\right),$$

这里$\xi=+1$或-1，视$p\equiv5$或$13\pmod{16}$而定；正整数J使 Pell 方程

$$x^2-16py^2=4,\ x,\ y\in Z$$

的最小解为ε_+^J，其中ε_+为$Q(\sqrt{p})$的全正基本单位。

这也可由定理3.3中取$k=4$，$d=p$而得出。

例 6 设有理素数$p\equiv1\pmod 8$使实二次域$Q(\sqrt{p})$的类数

为 1，则虚二次域 $Q(\sqrt{-2p})$ 的类数 $h(-2p)$ 满足

$$12h(-8p)=2\Psi(4\sqrt{p})-3\Psi(2\sqrt{p})+\Psi\left(\frac{2+\sqrt{p}}{4}\right)-\Psi\left(\frac{\sqrt{p}}{4}\right).$$

例 6 与例 7 可由定理 3.5 得出。

例 7 设有理素数 $p\equiv 5 \pmod 8$ 使实二次域 $Q(\sqrt{p})$ 的类数为 1，则虚二次域 $Q(\sqrt{-2p})$ 的类数 $h(-2p)$ 满足

$$\begin{aligned}12Jh(-2p)&=2\Psi(4\sqrt{p})-3\Psi(2\sqrt{p})\\&+\Psi\left(\frac{\sqrt{p}}{4}\right)-\Psi\left(\frac{2+\sqrt{p}}{4}\right)+2\xi_1\left(\Psi\left(\frac{1+\sqrt{p}}{16}\right)\right.\\&\left.-\Psi\left(\frac{7+\sqrt{p}}{16}\right)\right)+2\xi_2\left(\Psi\left(\frac{3+\sqrt{p}}{16}\right)-\Psi\left(\frac{5+\sqrt{P}}{16}\right)\right),\end{aligned}$$

这里正整数 J 使 ε_+^J 为 Pell 方程

$$x^2-64py^2=4$$

的最小解，ε_+ 为 $Q(\sqrt{p})$ 的全正基本单位。

$\xi_1=+1$，如 $p\equiv 21, 29 \pmod{32}$；

$\xi_1=-1$，如 $p\equiv 5, 13 \pmod{32}$；

$\xi_2=+1$，如 $p\equiv 5, 29 \pmod{32}$；

$\xi_2=-1$，如 $p\equiv 13, 21 \pmod{32}$。

§4 S.Chowla 的一个猜想

寻找类数 1 的实二次域这个问题中，一个最典型的例子是对具有形如 $d=4N^2+1$ 的判别式的实二次域 $K=Q(\sqrt{d})$，讨论其类数 h_K 等于 1 的可能性，其中 N 是一个正整数。容易验证，对这种形式的实二次域，有：

$h_K=1$，如 $N=1, 2, 3, 5, 7, 13$，也即相应地

$$d=5, 17, 37, 101, 197, 677.$$

利用 Siegel-Tatuzawa 定理可以证明，至多还可能再有一个类数为 1 的这种域。这一个可能的域，我们称为例外域。对此，S.

Chowla[10] 给出了下面的猜想。

猜想 (S.Chowla) 正好存在六个正整数 N，使判别式为 $4N^2+1$ 的实二次域 $K=Q(\sqrt{4N^2+1})$ 的类数等于 1。

根据 D.Goldfeld 的意见，这一猜想的最后解决有赖于椭圆曲线方面的进展，我们将在下一节中来阐明这一点。本节中，我们对 S.Chowla 的这一猜想作一些探讨，给出尽可能多的线索，最后还要证明上述的例外域的判别式大于 $10^{3.8\times10^7}$。

4.1　一些有关结果

本小节中首先列举一些我们在前面已经证明的结果，然后再证明另一些。因域的判别式 $d=4N^2+1$ 为素数时，域 $Q(\sqrt{d})$ 的类数才可能等于 1，所以可以只讨论形如 $p=4N^2+1$ 的素数 p。

定理 4.1　对素数 $p=4N^2+1$ (正整数 $N>1$)，实二次域 $Q(\sqrt{p})$ 的类数为 1 的充要条件是 N^2+x-x^2 $(2\leqslant x\leqslant N)$ 均为素数。

附注　Ankeny，Chowla 与 Hasse[2] 最初只证明了必要条件中的 N 为素数的结论。这个定理是我们[46—47] 在 1979 年首先证明的，后来 A.Mollin[76]，H.Yokoi[112] 等人又重复了这一工作。

定理 4.2　对素数 $p=4N^2+1$ (正整数 $N>1$)，实二次域 $Q(\sqrt{p})$ 的类数为 1 的充要条件是 $\bmod p$ 的最小素数二次剩余是 N，也即小于 N 的素数均在 $Q(\sqrt{p})$ 中惯性。

附注　S.Chowla 与 Friedlander[10] 最初只证明了必要条件，整个定理是我们[48] 首先在 1980 年证明的，以后 A.Mollin[77] 又重复了这一工作。

定理 4.3　设素数 $p=4N^2+1$ (正整数 $N>1$) 使实二次域 $Q(\sqrt{p})$ 的类数为 1，则虚二次域 $Q(\sqrt{-p})$ 的类数 $h(-p)=2N+4\left(\frac{-4}{N}\right)$，这里 $\left(\frac{-4}{N}\right)$ 是 Kronecker 符号。

上述三个定理我们已在 §2 中给出它们的证明。定理 4.3 也可由 §3.6 的例 5 得出。不妨设 $N>3$，故 N 为奇数。这时例 5 中

的 $p=4N^2+1\equiv 5 \pmod{16}$。故有

$$3h(-p)=\Psi(\sqrt{4p})+\Psi\left(\frac{3+\sqrt{p}}{8}\right)-\Psi\left(\frac{1+\sqrt{p}}{8}\right).$$

现今$\sqrt{4p}$，$\frac{5+\sqrt{p}}{8}$ 与$\frac{5+\sqrt{p}}{8}$的简单连分数展开式分别是

$$\sqrt{4p}=\sqrt{16N^2+4}=[4N,\ \overline{2N,\ 8N}];$$

$$\frac{1+\sqrt{p}}{8}=\begin{cases}\left[\frac{N-1}{4},\ \overline{2,1,1,1,\frac{N-3}{2},1,7,\frac{N-1}{2}}\right], & \text{如 } N\equiv 1 \pmod 4;\\ \left[\frac{N-3}{4},\ \overline{1,7,\frac{N-1}{2},2,1,1,1,\frac{N-3}{2}}\right], & \text{如 } N\equiv 3 \pmod 4;\end{cases}$$

$$\frac{5+\sqrt{p}}{8}=\begin{cases}\left[\frac{N-1}{4},\ \overline{1,7,\frac{N-1}{2},2,1,1,1,\frac{N-3}{2}}\right], & \text{如 } N\equiv 1 \pmod 4;\\ \left[\frac{N+1}{4},\ \overline{2,1,1,1,\frac{N-3}{2},1,7,\frac{N-1}{2}}\right], & \text{如 } N\equiv 3 \pmod 4.\end{cases}$$

于是有 $\Psi(\sqrt{4p})=6N$，以及

$$-\Psi\left(\frac{3+\sqrt{p}}{8}\right)=-\Psi\left(\frac{5+\sqrt{p}}{8}\right)=\Psi\left(\frac{1+\sqrt{p}}{8}\right)$$

$$=\begin{cases}-6, & \text{如 } N\equiv 1 \pmod 4;\\ 6, & \text{如 } N\equiv 3 \pmod 4,\end{cases}$$

故得$h(-p)=2N+4\left(\frac{-4}{N}\right)$，$N=2$，3 时，显然成立。定理已证明。

定理 4.4 如素数 $p=4N^2+1$ (正整数 $N>3$) 使实二次域 $Q(\sqrt{p})$的类数为 1，则虚二次域 $Q(\sqrt{-3p})$的类数 $h(-3p)$ 满足

$$3h(-3p)=\begin{cases}8N+10, & \text{如 } N\equiv 1 \pmod 3;\\ 8N-10, & \text{如 } N\equiv 2 \pmod 3.\end{cases}$$

证明

由 §3.6 的例 2, 可得

$$8h(-3p)=\Psi\left(\frac{1+3\sqrt{p}}{2}\right)-2\Psi\left(\frac{1+\sqrt{p}}{6}\right)+\Psi\left(\frac{3+\sqrt{p}}{6}\right).$$

现今$\frac{1+3\sqrt{p}}{2}$, $\frac{\pm1+\sqrt{p}}{6}$, $\frac{\pm3+\sqrt{p}}{6}$的简单连分数展开式分别是

$$\frac{1+3\sqrt{p}}{2}=\begin{cases}\left[3N,\overline{1,1,\frac{2(N-1)}{3},5,1,\frac{2(N-1)}{3}-1,1,5,\frac{2(N-1)}{3},1,1,6N-1}\right], & \text{如 } N\equiv1(\bmod 3);\\ \left[3N,\overline{1,1,\frac{2(N-2)}{3},1,5,\frac{2(N-2)}{3}+1,5,1,\frac{2(N-2)}{3},1,1,6N-1}\right], & \text{如 } N\equiv2(\bmod 3);\end{cases}$$

$$\frac{1+\sqrt{p}}{6}=\left[\frac{N-2}{3},\overline{1,5,\frac{2(N-2)}{3}+1,5,1,\frac{2(N-2)}{3},1,1,6N-1,1,1,\frac{2(N-2)}{3}}\right],\ \text{如 } N\equiv2(\bmod 3);$$

$$\frac{-1+\sqrt{p}}{6}=\left[\frac{N-1}{3},\overline{5,1,\frac{2(N-1)}{3}-1,1,5,\frac{2(N-1)}{3},1,1,6N-1,1,1,\frac{2(N-1)}{3}}\right],\ \text{如 } N\equiv1(\bmod 3);$$

$$\frac{3+\sqrt{p}}{6}=\left[\frac{N-2}{3}+1,\overline{5,1,\frac{2(N-2)}{3},1,1,6N-1,1,1,\frac{2(N-2)}{3},1,5,\frac{2(N-2)}{3}+1}\right],\ \text{如 } N\equiv2(\bmod 3);$$

$$\frac{-3+\sqrt{p}}{6}=\left[\frac{N-1}{3}-1,\overline{1,5,\frac{2(N-1)}{3},1,1,6N-1,1,1,\frac{2(N-1)}{3},5,1,\frac{2(N-1)}{3}-1}\right],\ \text{如 } N\equiv1(\bmod 3).$$

于是有：如 $N\equiv\pm1(\bmod 3)$, 则

$$-\Psi\left(\frac{1+\sqrt{p}}{6}\right)=-\Psi\left(\frac{\pm1+\sqrt{p}}{6}\right)=\Psi\left(\frac{3+\sqrt{p}}{6}\right)$$

$$=\Psi\left(\frac{\pm 3+\sqrt{p}}{6}\right)=\Psi\left(\frac{1+3\sqrt{p}}{2}\right)=\frac{16N\pm 20}{3}.$$

因此得到定理 4.4.

定理 4.5 如素数 $p=4N^2+1$（正整数 $N>2$）使实二次域 $Q(\sqrt{p})$ 的类数为 1, 则虚二次域 $Q(\sqrt{-2p})$ 的类数 $h(-2p)$ 满足

$$h(-2p)=\begin{cases}2(N+2), & \text{如 } N\equiv 1,\ 3 \pmod 8;\\ 2(N-2), & \text{如 } N\equiv 5,\ 7 \pmod 8.\end{cases}$$

证明 $N\leqslant 11$ 时容易验证. 下设 $N>11$. 由 §3.6 例 7 有

$$12h(-2p)=2\Psi(4\sqrt{p})-3\Psi(2\sqrt{p})+\Psi\left(\frac{\sqrt{p}}{4}\right)$$
$$-\Psi\left(\frac{2+\sqrt{p}}{4}\right)-2\Psi\left(\frac{1+\sqrt{p}}{16}\right)+2\Psi\left(\frac{3+\sqrt{p}}{16}\right)$$
$$-2\Psi\left(\frac{5+\sqrt{p}}{16}\right)+2\Psi\left(\frac{7+\sqrt{p}}{16}\right).$$

有关的简单连分数展开式如下:

$$4\sqrt{p}=[8N,\overline{N,16N}],\quad 2\sqrt{p}=[4N,\overline{2N,8N}],$$
$$\frac{\sqrt{p}}{4}=\left[\frac{N-1}{2},\overline{1,1,4N-1,1,1,N-1}\right],\quad \frac{2+\sqrt{p}}{4}=\left[\frac{N+1}{2},\overline{16N,N}\right],$$

$$\frac{1+\sqrt{p}}{16}=\begin{cases}\left[\dfrac{N-1}{8},\overline{5,3,\dfrac{N-5}{4},1,15,\dfrac{N-1}{4}}\right], & \text{如 } N\equiv 1 \pmod 8;\\[2ex] \left[\dfrac{N-3}{8},\overline{2,3,1,1,\dfrac{N-3}{4},5,3,\dfrac{N-3}{4}}\right], & \text{如 } N\equiv 3 \pmod 8;\\[2ex] \left[\dfrac{N-5}{8},\overline{1,2,4,1,\dfrac{N-5}{4},2,3,1,1,\dfrac{N-5}{4}}\right], & \text{如 } N\equiv 5 \pmod 8;\\[2ex] \left[\dfrac{N-7}{8},\overline{1,15,\dfrac{N-3}{4},1,2,4,1,\dfrac{N-7}{4}}\right], & \text{如 } N\equiv 7 \pmod 8,\end{cases}$$

$$\frac{-3+\sqrt{p}}{16}=\begin{cases}\left[\frac{N-9}{8},\overline{1,\ 15,\ \frac{N-1}{4},\ 5,\ 3,\ \frac{N-5}{4}}\right], & \text{如 } N\equiv 1 \pmod 8;\\ \left[\frac{N-3}{8},\overline{5,3,\frac{N-3}{4},\ 2,\ 3,\ 1,\ 1,\ \frac{N-3}{4}}\right], & \text{如 } N\equiv 3 \pmod 8;\\ \left[\frac{N-5}{8},\overline{2,3,1,1,\frac{N-5}{4},1,2,4,1,\frac{N-5}{4}}\right], & \text{如 } N\equiv 5 \pmod 8;\\ \left[\frac{N-7}{8},\overline{1,\ 2,\ 4,\ 1,\ \frac{N-7}{4},1,15,\frac{N-3}{4}}\right], & \text{如 } N\equiv 7 \pmod 8,\end{cases}$$

$$\frac{5+\sqrt{p}}{16}=\begin{cases}\left[\frac{N-1}{8},\overline{2,3,1,1,\frac{N-5}{4},1,2,4,1,\frac{N-5}{4}}\right], & \text{如 } N\equiv 1 \pmod 8;\\ \left[\frac{N-3}{8},\overline{1,2,4,1,\frac{N-7}{4},1,15,\frac{N-3}{4}}\right], & \text{如 } N\equiv 3 \pmod 8;\\ \left[\frac{N-5}{8},\overline{1,\ 15,\ \frac{N-1}{4},\ 5,\ 3,\ \frac{N-5}{4}}\right], & \text{如 } N\equiv 5 \pmod 8;\\ \left[\frac{N+1}{8},\overline{5,\ 3,\ \frac{N-3}{4},\ 2,\ 3,\ 1,\ 1,\frac{N-3}{4}}\right], & \text{如 } N\equiv 7 \pmod 8;\end{cases}$$

$$\frac{-7+\sqrt{p}}{16}=\begin{cases}\left[\frac{N-9}{8},\overline{1,2,4,1,\frac{N-5}{4},\ 2,3,1,1,\ \frac{N-5}{4}}\right], & \text{如 } N\equiv 1 \pmod 8;\\ \left[\frac{N-11}{8},\overline{1,\ 15,\ \frac{N-3}{4},\ 1,\ 2,4,1,\frac{N-7}{4}}\right], & \text{如 } N\equiv 3 \pmod 8;\\ \left[\frac{N-5}{8},\overline{5,\ 3,\ \frac{N-5}{4},\ 1,\ 15,\frac{N-1}{4}}\right], & \text{如 } N\equiv 5 \pmod 8;\end{cases}$$

$$\left\{\left[\frac{N-7}{8},\overline{2,\ 3,\ 1,\ 1,\ \frac{N-3}{4},5,\ 3,\ \frac{N-3}{4}}\right],\quad \text{如 } N\equiv 7(\bmod 8).\right.$$

于是

$$\Psi\left(4\sqrt{p}\right)=15N,\ \Psi(2\sqrt{p})=6N,\ \Psi\left(\frac{\sqrt{p}}{4}\right)=-3N,$$

$$\Psi\left(\frac{2+\sqrt{p}}{4}\right)=-15N,$$

$$\Psi\left(\frac{1+\sqrt{p}}{16}\right)=-15,\ +3,\ -3,\ 15,\ \text{依} N\equiv 1,\ 3,5,7(\bmod 8)$$

而定；

$$\Psi\left(\frac{3+\sqrt{p}}{16}\right)=\Psi\left(\frac{-3+\sqrt{p}}{16}\right)=-\Psi\left(\frac{1+\sqrt{p}}{16}\right);$$

$$\Psi\left(\frac{5+\sqrt{p}}{16}\right)=3,\ -15,\ 15,\ -3,\ \text{依 } N\equiv 1,\ 3,\ 5,\ 7(\bmod 8)$$

而定；

$$\Psi\left(\frac{7+\sqrt{p}}{16}\right)=\Psi\left(\frac{-7+\sqrt{p}}{16}\right)=-\Psi\left(\frac{5+\sqrt{p}}{16}\right).$$

因此有

$$h(-2p)=2(N\pm 2),$$

其中 $N\equiv 1,\ 3(\bmod 8)$ 时取 + 号；$N\equiv 5,\ 7(\bmod 8)$ 时取 − 号。定理证毕。

定理 4.6 除去 $N=1,\ 2,\ 3,\ 5,\ 7,\ 13$ 这六种情形之外，至多还可能再存在一个正整数 N，使素数 $p=4N^2+1$ 满足 $h(p)=1$，这里 $h(p)$ 表示实二次域 $K=Q(\sqrt{p})$ 的类数。并且这个可能的例外域的判别式 $p\geqslant 4.1\times 10^6$。

证明 K 的基本单位是 $\varepsilon_K=2N+\sqrt{p}$，由类数公式可知有

$$h(p)=\frac{\sqrt{p}L(1,\ \chi)}{2\log(2N+\sqrt{p})}\tag{6.75}$$

这里 $\chi(*)=\left(\frac{p}{*}\right)$ 为 Kronecker 符号。在第四章的定理 1.3 中取 $\varepsilon=(6\log 10)^{-1}$，则可知除去至多可能有一个例外情况以外，有

$$L(1,\ \chi)>\min\left(\frac{0.125}{\log p},\ \frac{14\varepsilon}{p^{\varepsilon}}\right),\ \text{如}\ p\geqslant 10^6. \qquad (6.76)$$

我们先设 $p\geqslant 4.1\times10^6$, 则由(6.75)与(6.76)可知，除去至多可能有一个例外情况以外，有

$$h(p)>\frac{\sqrt{p}}{2\log(2\sqrt{p})}\min\left(\frac{0.125}{\log p},\ \frac{14\varepsilon}{p^{\varepsilon}}\right). \qquad (6.77)$$

易见

$$\frac{0.125\sqrt{p}}{(\log p)(\log 4p)}\geqslant\frac{0.125\times\sqrt{4.1}\times10^3}{(\log(4.1\times10^6))\times\log(4\times4.1\times10^6)}$$

$$>1.0005>1,\ \text{如}\ p\geqslant4.1\times10^6,$$

$$\frac{14\varepsilon p^{\frac{1}{2}-\varepsilon}}{\log 4p}\geqslant\frac{14\times(4.1\times10^6)^{\frac{1}{2}-\frac{1}{6\log 10}}}{6(\log 10)\log(4\times4.1\times10^6)}>46,$$

$$\text{如}\ p\geqslant4.1\times10^6,$$

由此及(6.77)即知，至多可能有一个素数 $p=4N^2+1\geqslant4.1\times10^6$ (正整数 $N>1013$ 时即可成立)，使实二次域 $Q(\sqrt{p})$ 的类数 $h(p)=1$.

对于 $<4.1\times10^6$ 的素数 $p=4N^2+1$ (相当于正整数 $N\leqslant1012$)，可用已于上述定理 4.1—4.5 中证明了的充要条件(或者下列的定理 4.7)在计算机上验证出只有 $N=1,\ 2,\ 3,\ 5,\ 7,\ 13$ 这六种情况下才有 $h(p)=1$. 定理已证明.

定理 4.7　对素数 $p=4N^2+1$(N 为正整数)，实二次域 $K=Q(\sqrt{p})$ 类数为 1 的充要条件是

$$\sum_{x=0}^{N-1}\sigma(N^2-x-x^2)=\frac{N(2N^2+7)}{3}, \qquad (6.78)$$

这里 $\sigma(*)$ 是 $*$ 的正因子的和.

证明　因为(6.78)的左边是 $30\xi_K(-1)$. 故由本章定理 2.6 的(3)即得所需. 定理证毕.

4.2 例外域

本小节致力于证明下列的定理.

定理 4.8　设素数 $p=4N^2+1$(N 是正整数)使实二次域 $K=$

$Q(\sqrt{p})$ 的类数 $h(p)=1$，且 $p>677$，即 K 为 S. Chowla 猜想的例外域，则必有 $p>10^{3.8\times10^7}$。

证明 首先不难证明，对上述形状的素数 $p=4N^2+1$，必有 $h(p)>1$，如 $677<p<10^{14}$。以下设素数 $p=4N^2+1\geqslant10^{14}$，且有 $h(p)=1$，我们来证明 $p>10^{3.8\times10^7}$。K 的基本单位 $\varepsilon=2N+\sqrt{p}$，取 K 的一个整理想 $\mathfrak{A}=[1,\omega]$，$\omega=\dfrac{1+\sqrt{p}}{2}$。与 $\mathfrak{A}$ 对应的二元二次型是 $f(x,y)=x^2+xy-N^2y^2$。由第三章的(3.113)及 $h(p)=1$，可知有

$$2\zeta(s)L(s,\chi_p)=\sum_{\lambda\in\mathfrak{A}/\varepsilon}{}' \frac{1}{|\lambda\lambda'|^s},\ \mathrm{Re}s>1,\tag{6.79}$$

这里

$$\lambda=m\omega+n,\ \lambda'=m\omega'+n,\ \omega=\frac{1+\sqrt{p}}{2},$$
$$\omega'=\frac{1-\sqrt{p}}{2},\ m,n\in\mathbf{Z},$$

求和号上的"$'$"表示不计入 $(m,n)=(0,0)$ 的项；

$$\chi_p(*)=\left(\frac{*}{p}\right)$$

为 Legendre 符号。

由

$$\frac{\Gamma\left(\frac{1}{2}s\right)^2}{2\Gamma(s)}=\int_{-\infty}^{+\infty}\frac{dv}{(e^v+e^v)^s},\ \mathrm{Re}s>0\tag{6.80}$$

及(6.79)，我们有 $(\mathrm{Re}s>1)$

$$\zeta(s)L(s,\chi_p)\frac{\Gamma\left(\frac{1}{2}s\right)^2}{\Gamma(s)}=\sum_{\lambda\in\mathfrak{A}/\varepsilon}{}'\int_{-\infty}^{+\infty}\frac{dv}{(\lambda^2e^v+\lambda'^2e^{-v})^s}$$
$$=\sum_{\lambda\in\mathfrak{A}}{}'\int_{-\log\varepsilon}^{\log\varepsilon}\frac{dv}{Q_v(m,n)^s},\tag{6.81}$$

这里

$$Q_v(m,n)=\lambda^2e^v+\lambda'^2e^{-v}=A_vm^2+B_vmn+C_vn^2,$$
$$A_v=\omega^2e^v+\omega'^2e^{-v}=\left(\frac{1+\sqrt{p}}{4}\right)^2e^v+\left(\frac{1-\sqrt{p}}{4}\right)^2e^{-v},$$

$$B_v = 2(\omega e^v + w' e^{-v}) = (1+\sqrt{p})e^v + (1-\sqrt{p})e^{-v},$$

$$C_v = e^v + e^{-v}.$$

容易算出

$$B_v^2 - 4A_v C_v = -4p,$$

因此 $Q_v(m, n)$ 是一个判别式为 $-4p$ 的正定的实系数的二元二次型。由此及(6.81)有

$$\zeta(s)L(s, \chi_p)\frac{\Gamma\left(\frac{1}{2}s\right)^2}{2\Gamma(s)} = \int_{-\log \varepsilon}^{\log \varepsilon} M_v(s)dv, \ \mathrm{Re}s>1, \tag{6.82}$$

其中

$$M_v(s) = \frac{1}{2}\sum_{\substack{-\infty<m,n<+\infty\\(m,n)\neq(0,0)}} Q_v(m, n)^{-s} = \frac{1}{2}\sum_{(m,n)\in \mathbb{Z}^2}{}' Q_v(m, n)^{-s}, \tag{6.83}$$

这里求和号上的“′”表示不计入 $(m, n) = (0, 0)$ 的那一项。

由 Euler 求和公式(见潘承洞与潘承彪著《解析数论基础》)有($\mathrm{Re}s>1$)

$$\begin{aligned} M_v(s) &= \frac{\zeta(2s)}{(e^v+e^{-v})^s} + \sum_{m=1}^{\infty}\sum_{n=-\infty}^{+\infty} Q_v(m, n)^{-s} \\ &= \frac{\zeta(2s)}{(e^v+e^{-v})^s} + \sum_{m=1}^{\infty}\int_{-\infty}^{+\infty}\frac{dy}{Q_v(m, y)^s} \\ &\quad + \sum_{m=1}^{\infty}\int_{-\infty}^{+\infty} B_1(y)\frac{dQ_v(m, y)^{-s}}{dy}dy, \end{aligned} \tag{6.84}$$

这里 $B_1(y) = \{y\} - \frac{1}{2}$ 是 Bernoulli 多项式，我们还要用到 $B_2(y) = \{y\}^2 - \{y\} + \frac{1}{6}$，这里 $\{y\}$ 是 y 的小数部分。我们有

$$\sum_{m=1}^{\infty}\int_{-\infty}^{+\infty}\frac{dy}{Q_v(m, y)^s} = \frac{\sqrt{\pi}\,p^{\frac{1}{2}-s}}{C_v^{1-s}}\cdot\frac{\zeta(2s-1)\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)}, \tag{6.85}$$

在计算积分时，用了变量替换 $y_1 = \dfrac{mB_v + 2C_v y}{2m\sqrt{p}}$。用这一变量替换与分部积分法，可得

$$\int_{-\infty}^{+\infty} B_1(y)\frac{dQ_v(m, y)^{-s}}{dy}dy$$

$$=\frac{C_v^{s+1}}{p^{s+\frac{1}{2}}m^{2s+1}}\int_{-\infty}^{+\infty}\frac{B_2(y)}{2}\frac{d^2(y_1^2+1)^{-s}}{dy_1^2}dy_1$$

$$=\frac{C_v^{s+1}}{p^{s+\frac{1}{2}}m^{2s+1}}\left(\frac{1}{48}\int_{-\infty}^{+\infty}\frac{d^2(y_1^2+1)^{-s}}{dy_1^2}dy_1\right.$$

$$\left.+\int_{-\infty}^{+\infty}\frac{B_2(y)-\frac{1}{24}}{2}\frac{d^2(y_1^2+1)^{-s}}{dy_1^2}dy_1\right)$$

$$=\frac{C_v^{s+1}}{p^{s+\frac{1}{2}}m^{2s+1}}\left(\frac{-s}{48}\cdot\frac{2y_1}{(y_1^2+1)^{s+1}}\Bigg|_{y_1=-\infty}^{y_1=+\infty}\right.$$

$$\left.+\frac{\theta}{16}\int_{-\infty}^{+\infty}\left(\frac{2|s|}{(y_1^2+1)^{3/2}}+\frac{4|s(s+1)|y_1^2}{(y_1^2+1)^{5/2}}\right)dy_1\right)$$

$$=\frac{C_v^{s+1}}{p^{s+\frac{1}{2}}m^{2s+1}}\theta|s|\left(\frac{1}{4}+\frac{|s+1|}{6}\right), \text{ 如 } \mathrm{Re}s\geqslant\frac{1}{2}. \tag{6.86}$$

其中用到

$$\left|B_2(y)-\frac{1}{24}\right|\leqslant\frac{1}{8},$$

θ 是一个不是处处都相同但其绝对值总是小于等于 1 的复数。

所以，(6.84)—(6.86) 给出了 (6.84) 左边的函数在 $\mathrm{Re}s>\frac{1}{2}$ 中的解析开拓，在该处，该函数的唯一奇点是 $s=1$。并且可知当 $s=\frac{1}{2}+i\alpha(\alpha>0)$ 为 $\zeta(s)$ 的零点时，有

$$0=\zeta(1+2i\alpha)\int_{-\log\varepsilon}^{\log\varepsilon}C_v^{-\frac{1}{2}-i\alpha}dv$$

$$+\frac{\sqrt{\pi}\Gamma(i\alpha)}{\Gamma\left(\frac{1}{2}+i\alpha\right)}p^{-i\alpha}\zeta(2i\alpha)\int_{-\log\varepsilon}^{\log\varepsilon}C_v^{-\frac{1}{2}+i\alpha}dv$$

$$+\theta\left|\frac{1}{2}+i\alpha\right|\left(\frac{1}{4}+\frac{\left|\frac{3}{2}+i\alpha\right|}{6}\right)\frac{\zeta(2+2i\alpha)}{p^{1+i\alpha}}\int_{-\log\varepsilon}^{\log\varepsilon}C_v^{\frac{3}{2}+i\alpha}dv, \tag{6.87}$$

我们有

$$\int_{-\log s}^{\log s} C_v^{-\frac{1}{2}\mp i\alpha}\, dv = \int_{-\infty}^{+\infty} C_v^{-\frac{1}{2}\mp i\alpha}\, dv - 2\int_{\log s}^{+\infty} C_v^{-\frac{1}{2}\mp i\alpha}\, dv$$

$$= \frac{\Gamma\left(\frac{1}{4} \pm \frac{i}{2}\alpha\right)^2}{2\Gamma\left(\frac{1}{2} \pm i\alpha\right)} + 2\theta\int_{\log s}^{+\infty} C_v^{-\frac{1}{2}}\, dv,$$

这里用了(6.80)，在第二个积分作替换 $\varphi = \arcsin\dfrac{2}{e^v + e^{-v}}$，即有

$$\int_{-\log s}^{\log s} C_v^{-\frac{1}{2}\mp i\alpha}\, dv = \frac{\Gamma\left(\frac{1}{4} \pm \frac{i}{2}\alpha\right)^2}{2\Gamma\left(\frac{1}{2} \pm i\alpha\right)} + \theta\sqrt{2}\int_0^{\varphi_0} \frac{d\varphi}{\sqrt{\sin\varphi}},$$

其中 $\varphi_0 = \arcsin\dfrac{1}{\sqrt{p}}$，再用

$$\int_0^{\varphi_0} \frac{d\varphi}{\sqrt{\sin\varphi}} = 2\int_0^{\varphi_0} \frac{d\sqrt{\sin\varphi}}{\cos\varphi} \leqslant \frac{2}{\sqrt{1-p^{-1}}}\sqrt{\sin\varphi_0} = \frac{2p^{-0.25}}{\sqrt{1-p^{-1}}},$$

即得

$$\int_{-\log s}^{\log s} C_v^{-\frac{1}{2}\mp i\alpha}\, dv = \frac{\Gamma\left(\frac{1}{4} \pm \frac{i}{2}\alpha\right)^2}{2\Gamma\left(\frac{1}{2} \pm i\alpha\right)} + \theta\frac{2\sqrt{2}\,p^{-0.25}}{\sqrt{1-p^{-1}}}. \tag{6.88}$$

同理可得

$$\int_{-\log s}^{\log s} C_v^{\frac{3}{2}+i\alpha} = 2\theta\int_0^{\log s} C_v^{\frac{3}{2}}dv = 4\sqrt{2}\,\theta\int_{\varphi_0}^{\frac{\pi}{2}} \frac{d\varphi}{(\sin\varphi)^{5/2}}$$

$$= \theta\frac{8\sqrt{2}\,p^{\frac{3}{4}}}{3\sqrt{1-p^{-1}}}, \tag{6.89}$$

又由 Riemann ζ 函数的函数方程有

$$\Gamma(i\alpha)\zeta(2i\alpha) = \pi^{-\frac{1}{2}+2i\alpha}\,\Gamma\left(\frac{1}{2} - i\alpha\right)\zeta(1-2i\alpha). \tag{6.90}$$

这样，由(6.87)—(6.90)可得

$$\left(\frac{p}{\pi^2}\right)^{i\alpha} + \frac{\Gamma\left(\frac{1}{4} - \frac{\alpha}{2}i\right)^2\zeta(1-2\alpha i)}{\Gamma\left(\frac{1}{4} + \frac{\alpha}{2}i\right)^2\zeta(1+2\alpha i)}$$

$$= \theta 8\sqrt{2}\left|\frac{\Gamma\left(\frac{1}{2}+\alpha i\right)}{\Gamma\left(\frac{1}{4}+\frac{\alpha}{2}i\right)}\right|.$$

$$\left[1+\frac{1}{3}\sqrt{\frac{1}{4}+\alpha_2}\left(\frac{1}{4}+\frac{\sqrt{\frac{9}{4}+\alpha^2}}{6}\right)\right]\left|\frac{\zeta(2+2\alpha i)}{\zeta(1+2\alpha i)}\right|\frac{p^{-0.25}}{\sqrt{1-p^{-1}}}, \tag{6.91}$$

若 $\frac{1}{2}+i\alpha(\alpha>0)$ 是 $\zeta(s)$ 的一个零点。

$\zeta(s)$ 在上半平面上的虚部最小的三个零点 $\frac{1}{2}+i\alpha_j(j=1,2,3)$ 满足

$$14.134725141<\alpha_1<14.134725142,$$
$$21.022039638<\alpha_2<21.022039639,$$
$$25.010857<\alpha_3<25.010859.$$

我们不难算出以下诸式：

$$|\zeta(1+2\alpha_j i)|>\begin{cases}1.948757, & 如\ j=1;\\ 0.830962, & 如\ j=2;\\ 0.544301347, & 如\ j=3,\end{cases}$$

$$|\zeta(2+2\alpha_j i)|<\begin{cases}1.4229, & 如\ j=1;\\ 0.9162, & 如\ j=2;\\ 0.7892, & 如\ j=3,\end{cases}$$

$$\log\left|\Gamma\left(\frac{3}{4}+\frac{\alpha_j}{2}i\right)\right|<\begin{cases}-9.6937176, & 如\ j=1;\\ -15.0036975, & 如\ j=2;\\ -18.093048, & 如\ j=3,\end{cases}$$

$$\left|\Gamma\left(\frac{1}{2}+\alpha_j i\right)\right|=\sqrt{\frac{2\pi}{e^{\pi\alpha_j}+e^{-\pi\alpha_j}}}$$

$$>\begin{cases}5.708835\times10^{-10}, & 如\ j=1;\\ 1.143149\times10^{-14}, & 如\ j=2;\\ 2.1725892\times10^{-17}, & 如\ j=3.\end{cases}$$

由 Γ 函数乘积公式有

$$\left|\frac{\Gamma\left(\frac{1}{2}+i\alpha\right)}{\Gamma\left(\frac{1}{4}+\frac{\alpha}{2}i\right)^2}\right| = \frac{1}{2\pi}\left|\frac{\Gamma\left(\frac{3}{4}+\frac{\alpha}{2}i\right)^2}{\Gamma\left(\frac{1}{2}+\alpha i\right)}\right|.$$

这样，由(6.91)不难算出，当 $p\geqslant 10^{14}$ 时，有

$$\left(\frac{p}{\pi^2}\right)^{i\alpha_j}+\frac{\Gamma\left(\frac{1}{4}-\frac{\alpha_j}{2}i\right)^2\zeta(1-2\alpha_j i)}{\Gamma\left(\frac{1}{4}+\frac{\alpha_j}{2}i\right)^2\zeta(1+2\alpha_j i)}$$

$$=\theta\times\begin{cases}245.257p^{-\frac{1}{4}}, \text{ 如 } j=1;\\ 2765.11p^{-\frac{1}{4}}, \text{ 如 } j=2;\\ 5466.34p^{-\frac{1}{4}}, \text{ 如 } j=3\end{cases} \tag{6.92}$$

因此当 $p\geqslant 6.4\times 10^{64}$ 时，有

$$\alpha_j\log\frac{p}{\pi^2}=a_j+2\pi x_j+\theta b_j 10^{-14},\ j=1,\ 2, \tag{6.93}$$

其中 x_1, x_2 为非负的有理整数；$b_1=1.55$, $b_2=17.39$;

$$a_j\equiv\pi-4\arg\Gamma\left(\frac{1}{4}+\frac{\alpha_j}{2}i\right)-2\arg\zeta(1+2\alpha_j i)\pmod{2\pi},$$

$$0\leqslant a_j<2\pi,\ j=1\ \ 2. \tag{6.94}$$

由

$$\frac{2}{\pi}\arg\Gamma\left(\frac{1}{4}+\frac{i}{2}\alpha_j\right)$$

$$=\begin{cases}4.04988908734575785+2.1\times 10^{-13}\theta, \text{ 如 } j=1;\\ 8.80040877886703\qquad +2.1\times 10^{-13}\theta, \text{ 如 } j=2,\end{cases}$$

$$\frac{1}{\pi}\arg\zeta(1+2i\alpha_j)$$

$$=\begin{cases}-0.108452737083095+10^{-10}\theta, \text{ 如 } j=1;\\ 0.067103865503910+10^{-10}\theta, \quad \text{ 如 } j=2,\end{cases}$$

以及(6.94)即得

$$\frac{a_j}{2\pi}=\begin{cases}0\ \ 55856364973733715+1.003\times 10^{-10}\theta, \text{ 如 } j=1;\\ 0.63248735562906\qquad +1.003\times 10^{-10}\theta, \text{ 如 } j=2,\end{cases}$$

由此，并从(6.93)中消去 $\log\frac{p}{\pi^2}$，即得

$$x_2=\frac{\alpha_2}{\alpha_1}x_1+a+y, \tag{6.95}$$

其中

$$a=\frac{1}{2\pi}\left(\frac{\alpha_2}{\alpha_1}a_1-a_2\right)=0.19824313745544+1.76\times10^{-10}\theta,$$

$$y=\frac{1}{2\pi}\left(\frac{\alpha_2}{\alpha_1}b_1+b_2\right)\times10^{-14}\theta=3.135\times10^{-14}\theta.$$

这里用到

$$\frac{\alpha_2}{\alpha_1}=1.487262003892890048+10^{-18}\theta.$$

再用

$$13.583601172491450432=9\frac{\alpha_2}{\alpha_1}+a+1.77\times10^{-10}\theta,$$

与(6.95)相减,即有

$$x_2-14=\frac{\alpha_2}{\alpha_1}(x_1-9)-b+1.78\times10^{-10}\theta, \tag{6.96}$$

$$b=0.41639882751.$$

由 $p\geqslant6.4\times10^{64}$ 及(6.93)可知有

$$x_1\geqslant330. \tag{6.97}$$

取

$$p_0=372629826,\ q_0=250547533,$$

即知 p_0 与 q_0 互素,以及

$$\frac{p_0}{q_0}=1.4872620038928900569l\cdots, \tag{6.98}$$

由(6.98)即知有

$$\left|\frac{p_0}{q_0}-\frac{\alpha_2}{\alpha_1}\right|<10^{-17}. \tag{6.99}$$

令有理整数 Q 与 $R(0\leqslant R<q_0)$ 使

$$\frac{p_0}{q_0}(x_1-9)=Q+\frac{R}{q_0},$$

则有

$$p_0(x_1-9)\equiv R(\bmod q_0), \tag{6.100}$$

$$x_2 - Q - 14 = \left(\frac{\alpha_2}{\alpha_1} - \frac{p_0}{q_0}\right)(x_1 - 9) + \frac{R}{q_0} - b + 1.78 \times 10^{-10}\theta, \tag{6.101}$$

$$bq_0 = 104327698.97672303283. \tag{6.102}$$

当 $R \neq 104327699$ 时，由(6.102)即知

$$\left|\frac{R}{q_0} - b\right| > 3.898 \times 10^{-9}, \tag{6.103}$$

如这时还有 $x_1 < 199555305$ 的话，则由(6.99)、(6.101)和(6.103)有

$$|x_2 - Q - 14| > 3.898 \times 10^{-9} - (x_1 - 9) \times 10^{-17} - 1.78 \times 10^{-10} > 0,$$

注意已知 $x_1 \geqslant 330$，同时也有

$$|x_2 - Q - 14| \leqslant (x_1 - 9) \times 10^{-17} + (1 - b) + 1.78 \times 10^{-10} < 1.$$

这两个不等式与 $x_2 - Q - 14$ 是有理整数矛盾。因此这时应有 $x \geqslant 199555305$。而当 $R = 104327699$ 时，用(6.100)可得

$$p_0(x_1 - 9) \equiv 104327699 (\bmod q),$$

由此及

$$64794022p_0 - 9636568q_0 = 1$$

即得

$$x_1 \equiv 199555305 (\bmod 250547533),$$

结合(6.97)即 $x_1 \geqslant 330$，也得 $x_1 \geqslant 199555305$。

所以 $\chi_1 \geqslant 199555305$ 总是成立的，因此由(6.93)有

$$p \geqslant \pi^2 \exp\left(\frac{(0.5585 + 199555305)2\pi - 1.55 \times 10^{-14}}{14.134726}\right) > 10^{3.8 \times 10^7}.$$

以上证明了当 $p \geqslant 6.4 \times 10^{64}$ 时，必有 $p > 10^{3.8 \times 10^7}$。

如有 $5.8 \times 10^{26} \leqslant p < 6.4 \times 10^{64}$，则有

$$133 \leqslant x_1 \leqslant 329,\ x_2 = \frac{\alpha_2}{\alpha} x_1 + a + y_1,\ |y_1| \leqslant 0.00010151, \tag{6.104}$$

$$x_2 - 14 = \frac{\alpha_2}{\alpha_1}(x_1 - 9) - b + y_1 + 1.78 \times 10^{-10}\theta. \tag{6.105}$$

令 $p_1=409$, $q_1=275$, 则

$$\left|\frac{\alpha_2}{\alpha_1}-\frac{p_1}{q_1}\right|<1.0724\times10^{-5}. \qquad (6.106)$$

令有理整数 Q_1, $R_1(0\leqslant R_1<q_1)$使

$$\frac{p_1}{q_1}(x_1-9)=Q_1+\frac{R_1}{q_1},$$

则由(6.104)—(6.106)有

$$|x_2-14-Q_1|=\left|\left(\frac{\alpha_2}{\alpha_1}-\frac{p_1}{q_1}\right)(x_1-9)+\frac{R_1}{q}-b+y_1+1.78\right.$$
$$\left.\times10^{-10}\theta\right|<321\times1.0724\times10^{-5}+1-b+0.00010152<1,$$

但 x_2-14-Q_1 是有理整数, 故 $x_2-14-Q_1=0$, 从而

$$\left|\frac{R_1}{q_1}-b\right|=\left|\left(\frac{\alpha_2}{\alpha_1}-\frac{p_1}{q_1}\right)(x_1-9)+y_1+1.78\times10^{-10}\theta,\right.$$

因此

$$|R_1-bq_1|\leqslant275\times321\times1.0724\times10^{-5}$$
$$+0.00010152\times275=0.9720411,$$

但 $bq_1=114.50952560275$, 所以我们有

$$R_1=114 \text{ 或 } 115. \qquad (6.107)$$

再由

$$p_1(x_1-9)\equiv R_1(\bmod q_1),\ 39p_1-58q_1=1,$$

有

$$x_1\equiv9+39R_1(\bmod 275). \qquad (6.108)$$

由(6.107)与(6.108)得到 $x_1\equiv55$ 或 $94(\bmod 275)$ 这与 $133\leqslant x_1\leqslant329$ 矛盾。因此 $5.8\times10^{26}\leqslant p<6.4\times10^{64}$ 是不可能的。

如有 $2\times10^{19}\leqslant p<5.8\times10^{26}$, 则有 $95\leqslant x_1\leqslant132$, 以及

$$x_2=\frac{\alpha_2}{\alpha_1}x_1+a+y_2,\ |y_2|\leqslant0.008859,$$

可有

$$x_2-14-Q_1=\left(\frac{\alpha_2}{\alpha_1}-\frac{p_1}{q_1}\right)(x_1-9)+\frac{R_1}{q}-b$$
$$+y_2+1.78\times10^{-10}\theta,$$

易见 $|x_2-14-Q_1|<1$, 故 $x_2-14-Q=0$, 从而可得

$$|R_1 - bq_1| \leqslant 2.7992393,\ 112 \leqslant R_1 \leqslant 117.$$

所以

$$x_1 \equiv 16,\ 55,\ 94,\ 133,\ 172,\ 252 \pmod{275},$$

这与 $95 \leqslant x_1 \leqslant 132$ 矛盾，因此 $2\times10^{19} \leqslant p < 5.8\times10^{26}$ 不可能。

如有 $10^{18} \leqslant p < 2\times10^{19}$，则有 $88 \leqslant x_1 \leqslant 94$ 及

$$x_2 = \frac{\alpha_2}{\alpha_1}x_1 + a + y_3,\ |y_3| \leqslant 0.015752397,$$

可有

$$x_4 - 14 - Q_1 = \left(\frac{\alpha_2}{\alpha_1} - \frac{p_1}{q_1}\right)(\chi - 9) + \frac{R_1}{q_1} - b$$
$$+ y_3 + 1.78\times10^{-10}\theta,$$

易见 $|x_2 - 14 - Q_1| < 1$，故 $x_2 - 14 - Q_1 = 0$。从而

$$|R_1 - bq_1| < 4.5887,\ 111 \leqslant R_1 \leqslant 119,$$

与此相应的只可能是 $x_1 = 94,\ R_1 = 115$。于是

$$p > 1.7737\times10^{19}.$$

用

$$18.69345084 < \arg\Gamma\left(\frac{1}{4} + \frac{\alpha_3}{2}\mathrm{i}\right) < 18.69345993,$$

$$-0.956746798 < \arg\zeta(1 + 2x_3\mathrm{i}) < -0.956631696 \pmod{2\pi},$$

可得与 $j=3$ 时的 α_3 满足

$$5.67924001 < \alpha_3 < 5.67950658,$$

以及由此而得到的下列等式

$$x_3 = \frac{\alpha_3}{\alpha_1}x_1 + a' + y',\ |y'| < 0.0145, \tag{6.109}$$

其中

$$1.7694618571 < \frac{\alpha_3}{\alpha_1} < 1.7694619987, \tag{6.110}$$

$$0.0844603415 < a' < 0.084478033. \tag{6.111}$$

对一个实数 x，令 $<x>$ 为 x 与离 x 最近的有理整数的距离，则由 $\chi_1 = 94$，即由 (6.109) 有

$$<94\frac{\alpha_3}{\alpha_1} + a'> = <x_3 - y'> < 0.0145,$$

但由(6.110)与(6.111)有$<94\frac{\alpha_3}{\alpha_1}+a'>>0.4$，得出矛盾。这证明了不可能有$10^{18}\leqslant p<2\times10^{19}$。

如有$10^{16}\leqslant p<10^{18}$，则有$77\leqslant x\leqslant87$及

$$x_2=\frac{\alpha_2}{\alpha_1}x_1+a+y_4,\quad |y_4|<0.049813451.$$

用与上相同的方法，可以证明只有$x_1=84$或86。这时应有

$$x_3=\frac{\alpha_3}{\alpha_1}x_1+a'+y_1',\quad |y_1'|<0.06641.$$

于是

$$<\frac{\alpha_3}{\alpha_1}x_1+a'><0.06641. \tag{6.112}$$

由(6.110)与(6.111)易得$x_1=84$或86时，有

$$<\frac{\alpha_3}{\alpha_1}x_1+\alpha'>>0\cdot2,$$

这与(6.112)矛盾。因此$10^{16}\leqslant p<10^{18}$也不可能。

如有$10^{14}\leqslant p<10^{6}$，则有$67\leqslant x_1\leqslant76$，以及

$$x_2=\frac{\alpha_2}{\alpha_1}x_1+a+y_5,\quad |y_5|<0.15752397,$$

同理可证只有$x_1=67$或76。这时再用

$$x_3=\frac{\alpha_3}{\alpha_1}x_1+a'+y_2',\quad |y_2'|<0.297,$$

与上同样可以证明会产生一对矛盾：

$$0.3<<\frac{\alpha_3}{\alpha_1}x_1+a'><0.297,$$

因此$10^{14}\leqslant p<10^{16}$也不可能。

这样，我们就完成了$p>10^{3.8\times10^9}$的证明。定理证毕。

§5 Goldfeld 定理

本节中，我们要在存在一条具有特殊性质的椭圆曲线E的假设下，来证明可以得到关于实二次域$K=Q(\sqrt{d})$的类数$h(d)$的如下形式的有效估计：当$d>c_1$时，有

$$h(d) > c_2 \frac{(\log d)^{g-\mu-1}\exp\left(-21g^{\frac{1}{2}}(\log\log d)^{\frac{1}{2}}\right)}{\log\varepsilon},$$

这里 g 是椭圆曲线 E 的秩；d，ε 分别是 K 的判别式与基本单位；c_1，c_2 是仅与 E 有关的可计算的有效正常数；当 d 与 E 的导子 N 互素时，$\mu=1, 2$ 如下决定之：$\chi_d(-N)=(-1)^{g-\mu}$，这里

$$\chi_d(*)=\left(\frac{d}{*}\right)$$

是 Kronecker 符号，而当 d 与 N 不互素时，情况要复杂一些。这就是所谓的 Goldfeld 定理。

我们先给出一些引理，然后再证明 Goldfeld 定理。

5.1 一些引理

引理 5.1 设 A, B, C 为实数，$A>0$，$4AC-B^2=\Delta>0$。则对任意的实数 $\chi>0$，有

$$S(\chi)\overset{\text{def}}{=\!=}\sum_{\substack{Am^2+Bmn+Cn^2\leqslant\chi\\(m,n)\in Z\times Z^*}}1=\frac{2\pi\chi}{\sqrt{\Delta}}+4\theta\sqrt{\frac{A\chi}{\Delta}}-4\rho\sqrt{\frac{\chi}{A}},$$

这里和以后出现的 θ，ρ 均为实数，它们满足 $|\theta|\leqslant1$，与 $0\leqslant\rho\leqslant1$，且不一定都相同。

证明 $S(\chi)$ 即为满足条件

$$(2Am+Bn)^2+\Delta n^2\leqslant4A\chi,\ (m,n)\in Z\times Z^*$$

的有理整数 (m, n) 的组数。上述条件等价于

$$-\sqrt{4A\chi-\Delta n^2}-Bn\leqslant2Am\leqslant\sqrt{4A\chi-\Delta n^2}-Bn,$$

$$m,\ n\in Z,\ 0<|n|\leqslant\lambda=2\sqrt{\frac{A\chi}{\Delta}}.$$

因此有

$$\begin{aligned}S(\chi)&=\frac{2}{A}\sum_{0<n\leqslant\lambda}\sqrt{4A\chi-\Delta n^2}+2\theta\sum_{1\leqslant n\leqslant\lambda}1\\&=\frac{2\sqrt{\Delta}}{A}\sum_{0<n\leqslant\lambda}\sqrt{\lambda^2-n^2}+2\theta\lambda\\&=\frac{2\sqrt{\Delta}}{A}\left(\frac{\pi}{4}\lambda^2-\rho\lambda\right)+2\theta\lambda,\end{aligned}$$

以 λ 的值代入，即得引理。

引理 5.2 设 $K=Q(\sqrt{d})$ 为一个给定的实二次域，d 为 K 的判别式，$\zeta_K(s)$ 为 K 的 Dedekind ζ 函数。则对于 $s=\sigma+it$，$\sigma=\mathrm{Re}s>\frac{1}{2}$，有

$$\frac{\Gamma\left(\frac{s}{2}\right)^2}{\Gamma(s)}\zeta_K(s)=\sum_{\mathfrak{A}=\left[a,\frac{-b+\sqrt{d}}{2}\right]}\sum_{n=0}^{M-1}\left(2\zeta(2s)\int_{H_n\delta_n}^{H_{n+1}\delta_n}(A_n^*)^{-s}\frac{d\varphi}{\varphi}\right.$$

$$\left.+\frac{\pi}{\sqrt{d}}\frac{s}{s-1}\int_{H_n\delta_n}^{H_{n+1}\delta_n}\left(\frac{d}{A_n^*}\right)^{1-s}\frac{d\varphi}{\varphi}\right)+R_1(s),\tag{6.113}$$

其中

$$|R_1(s)|\leqslant\frac{4|s|}{\sigma-\frac{1}{2}}\sum_{\mathfrak{A}=\left[a,\frac{-b+\sqrt{d}}{2}\right]}\sum_{n=0}^{M-1}\int_{H_n\delta_n}^{H_n\delta_{n+1}}\left(\frac{1}{2}\left(\frac{A_n^*}{d}\right)^{\sigma}\right.$$

$$\left.+\frac{(A_n^*)^{\sigma-1}}{d^{\sigma-\frac{1}{2}}}\right)\frac{d\varphi}{\varphi},$$

这里 $\mathfrak{A}=\left[a,\ \frac{-b+\sqrt{d}}{2}\right]$ 跑过 K 的理想类群 $\mathscr{C}_K$ 的一个完全代表元组，并且满足下列条件：

$|b|\leqslant a\leqslant c$，$d=b^2+4ac$，$a$，$b$，$c\in Z$，$g.c.d.(a,\ b,\ c)=1$；

$\alpha=\frac{b+\sqrt{d}}{2a}$ 的简单连分数展开式为

$$\alpha=[a_0,\ \overline{a_1,\ \cdots,\ a_k}],$$

这里 $\overline{a_1,\ \cdots,\ a_k}$ 为基本周期，命它的第 n 个完全商和第 n 个渐近分数分别是

$$\alpha_n=\frac{P_n+\sqrt{d}}{2Q_n},\quad \frac{p_n}{q_n},\ n\geqslant 0;$$

当 $k=1$ 时，$M=1$，$H_0=\frac{a}{\sqrt{d}}$，$H_1=\frac{a}{\sqrt{d}}\varepsilon^2$，$\varepsilon$ 是 K 的基本单位。当 k 为奇数且 $k\geqslant 3$ 时，$M=k$，$H_0=\frac{a}{\sqrt{d}}$，$H_k=\frac{a}{\sqrt{d}}\varepsilon^2$，

$$H_n=\frac{\sqrt{d}}{2b}\left(q_{n-1}^2+\sqrt{q_{n-1}^4-\frac{4a^2}{d}}\right)(1\leqslant n\leqslant k-1).$$

当 k 为偶数时，$M=k+1$，$H_0=\frac{a}{\sqrt{d}}$，$H_{k+1}=\frac{a}{\sqrt{d}}\varepsilon^2$，

$$H_n=\frac{\sqrt{d}}{2b}\left(q_{n-1}^2+\sqrt{q_{n-1}^4-\frac{4a^2}{d}}\right)(1\leqslant n\leqslant k);$$

$$A_n^*=Q_n\left(\varphi+\frac{1}{\varphi}\right)\leqslant 5\sqrt{d}\ (0\leqslant n\leqslant M-1);$$

$$\delta_0=1,\ \delta_n=\left|\frac{q_{n-1}\alpha-p_{n-1}}{q_{n-1}\alpha'-p_{n-1}}\right|(1\leqslant n\leqslant M-1),\ \alpha'=\frac{b-\sqrt{d}}{2a}.$$

证明 令 $\mathfrak{A}$ 所属的理想类为 $\mathcal{A}^{-1}$。则对应

$$\mathfrak{B}\mapsto\mathfrak{B}\mathfrak{A}=(\lambda)$$

是理想 $\mathfrak{B}\in\mathcal{A}$ 与由 $\lambda\in\mathfrak{A}$ 生成的主理想 (λ) 之间的一个一一对应。λ_1 与 λ_2 定义同一个主理想当且仅当 $\lambda_1=\eta\lambda_2$，这里 $\eta\in U=\{\pm\varepsilon^n|n\in\mathbb{Z}\}$，$U$ 是 K 的单位群，ε 为 K 的基本单位。这样 $\mathcal{A}$ 的 ζ 函数

$$\zeta_K(s|\mathcal{A})=N(\mathfrak{A})^s\sum_{\substack{\lambda\in\mathfrak{A}/U\\ \lambda\neq 0}}\frac{1}{|\lambda\lambda'|^s},\ \operatorname{Re}s>1.$$

易见

$$N(\mathfrak{A})=a,\ \lambda=am+\frac{b+\sqrt{d}}{2}n,$$

$$\lambda'=am+\frac{b-\sqrt{d}}{2}n,\ m,\ n\in\mathbb{Z}.$$

又

$$\frac{1}{|\lambda\lambda'|^s}=\frac{2\Gamma(s)}{\Gamma\left(\frac{s}{2}\right)^2}\int_{-\infty}^{+\infty}\frac{d\varphi}{(\lambda^2e^{\varphi}+(\lambda')^2e^{-\varphi})^s},$$

于是有

$$\zeta_K(s|\mathcal{A})=\frac{2\Gamma(s)}{\Gamma\left(\frac{s}{2}\right)^2}N(\mathfrak{A})^s\sum_{\substack{\lambda\in\mathfrak{A}/U\\ \lambda\neq 0}}\int_{-\infty}^{+\infty}\frac{d\varphi}{(\lambda^2e^{\varphi}+(\lambda')^2e^{-\varphi})^s}$$

$$=\frac{\Gamma(s)}{\Gamma\left(\frac{s}{2}\right)^2}N(\mathfrak{A})^s\sum_{\substack{\lambda\in\mathfrak{A}\\ \lambda\neq 0}}\int_{\log\xi}^{\log\xi+2\log\varepsilon}\frac{d\varphi}{(\lambda^2e^{\varphi}+(\lambda')^2e^{-\varphi})^s},$$

其中 ξ 为任一个实数，再作变量替换 $\varphi\mapsto\log\varphi$，即有

$$\frac{\Gamma\left(\frac{s}{2}\right)^2}{\Gamma(s)}\zeta_K(s)=\sum_{\mathfrak{A}=\left[a,\frac{-b+\sqrt{d}}{2}\right]}\int_{\xi}^{\xi\varepsilon^2}\sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{+\infty}$$

$$(Am^2+Bmn+Cn^2)^{-s}\frac{d\varphi}{\varphi},\tag{6.114}$$

这里 $B^2-4AC=-4d$，更确切些，有：

$$A=a\left(\varphi+\frac{1}{\varphi}\right),\ B=2a\left(\alpha\varphi+\frac{\alpha'}{\varphi}\right),\ C=a\left(\alpha^2\varphi+\frac{\alpha'^2}{\varphi}\right).$$

我们考虑Epstein zeta函数

$$\sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{+\infty}(Am^2+Bmn+Cn^2)^{-s}=d^{-\frac{s}{2}}E(z,s),\ \mathrm{Re}s>1,$$

这里的Eisenstein级数

$$E(z,s)=y^s\sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{+\infty}|m+nz|^{-2s},\ \mathrm{Re}s>1.$$

其中

$$z=x+iy=\frac{\alpha'+\alpha\varphi^2}{1+\varphi^2}+i\frac{\sqrt{d}}{a}\cdot\frac{\varphi}{1+\varphi^2}.$$

易见有

$$|b|\leqslant a<\frac{\sqrt{d}}{2}.\tag{6.115}$$

当 $k=1$ 时，$\alpha=\frac{b+\sqrt{d}}{2a}=[a_0,\ \overline{a}_1]=\frac{2a_0-a_1+\sqrt{a_1^2+4}}{2}$，故 $a=1$，$b=0$ 或 ±1，$d=a_1^2+4$，$a_1=2a_0$ 或 $2a_0\pm1$。$\varepsilon=p_0+q_0\frac{\sqrt{d}-b}{2a}=\frac{a_1+\sqrt{d}}{2}<\sqrt{d}=\frac{\sqrt{d}}{a}$。

当 k 奇且大于等于3时，$\varepsilon\varepsilon'=-1$，这里 ε' 是 ε 的共轭元，由

$$\varepsilon=p_{k-1}+q_{k-1}\frac{\sqrt{d}-b}{2a},$$

即知有

$$\varepsilon-\frac{\sqrt{d}}{a}q_{k-1}=p_{k-1}-q_{k-1}\frac{\sqrt{d}+b}{2a}=\varepsilon'<0.$$

再由

$$q_{k-1}-q_{k-2}\geqslant q_{k-3}\geqslant 1>\frac{1}{2}>\frac{a}{\sqrt{d}},$$

即知

$$\frac{\sqrt{d}}{a}(q_{k-1}-q_{k-2})>1>\frac{1}{\varepsilon}=-\varepsilon'=\frac{\sqrt{d}}{a}q_{k-1}-\varepsilon,$$

于是有

$$q_{k-2}<\frac{a}{\sqrt{d}}\varepsilon<q_{k-1}, \text{ 如 } k \text{ 奇且 } k\geqslant 3. \qquad (6.116)$$

当 k 偶时，由 $\varepsilon\varepsilon'=1$ 及

$$\varepsilon-\frac{\sqrt{d}}{a}q_{k-1}=\varepsilon'>0,$$

即知 $\varepsilon>\frac{\sqrt{d}}{a}q_{k-1}$，再由

$$q_k-q_{k-1}\geqslant q_{k-2}\geqslant 1>\frac{1}{2}+\frac{1}{4}>\frac{a}{\sqrt{d}}+\frac{1}{4},$$

即知

$$\frac{\sqrt{d}}{a}\left(q_k-q_{k-1}-\frac{1}{4}\right)>1>\frac{1}{\varepsilon}=\varepsilon'=\varepsilon-\frac{\sqrt{d}}{a}q_{k-1},$$

故得

$$q_{k-1}<\frac{a}{\sqrt{d}}\varepsilon<q_k-\frac{1}{4}, \text{ 如 } k \text{ 偶}. \qquad (6.117)$$

命

$$H'_n=\frac{\sqrt{d}}{2a}\left(q_n^2+\sqrt{q_n^4-\frac{4a^2}{d}}\right)(n\geqslant 0)$$

由(6.115)可知 H'_n 为一个实数。令 M_0 为最小的非负整数，它使

$$H'_{M_0}\geqslant\frac{a}{\sqrt{d}}\varepsilon^2.$$

不难证明，若有

$$H'_n>\frac{a}{\sqrt{d}}\varepsilon^2,$$

则必有 $q_n>\frac{a}{\sqrt{d}}\varepsilon$；反之，若有

$$q_n>1 \text{ 及 } H'_n<\frac{a}{\sqrt{d}}\varepsilon^2$$

则必有$q_n-\frac{1}{4}<\frac{a}{\sqrt{d}}\varepsilon$. 分别考虑$k$奇或偶并用(6.116)及(6.117)即可知有$M_0=M-1$, 这里的$M$已在引理中定义。由此不难证明,引理中定义的$M$, $H_n(0\leqslant n\leqslant M)$有下述性质

$$\frac{a}{\sqrt{d}}=H_0<H_1<\cdots<H_{M-1}<\frac{a}{\sqrt{d}}\varepsilon^2=H_M. \qquad (6.118)$$

取(6.114)中的$\xi=\frac{a}{\sqrt{d}}$, 即有

$$\frac{\Gamma\left(\frac{s}{2}\right)^2}{\Gamma(s)}\zeta_K(s)=\sum_{\mathfrak{A}=\left[a,\frac{-b+\sqrt{d}}{2}\right]}\sum_{n=0}^{M-1}\int_{H_n}^{H_{n+1}}d^{-\frac{s}{2}}E(z,s)\frac{d\varphi}{\varphi}. \qquad (6.119)$$

对$n=0$, $H_0=\frac{a}{\sqrt{d}}$, $H_1\leqslant\frac{\sqrt{d}}{a}$, $\delta_0=1$, 此时令

$$z_0^*=z,$$

可见,当$H_0\delta_0\leqslant\varphi\leqslant H_1\delta_0$时,有

$$\operatorname{Im}z_0^*=\operatorname{Im}z=\frac{\sqrt{d}}{a}\cdot\frac{1}{\varphi+\frac{1}{\varphi}}\geqslant\frac{\sqrt{d}}{a}\cdot\frac{1}{\frac{\sqrt{d}}{a}+\frac{a}{\sqrt{d}}}$$

$$=\frac{1}{1+\left(\frac{a}{\sqrt{d}}\right)^2}\geqslant\frac{4}{5}>\frac{1}{5},$$

并有

$$\int_{H_0}^{H_1}d^{-\frac{s}{2}}E(z,s)\frac{d\varphi}{\varphi}=\int_{H_0\delta_0}^{H_1\delta_0}d^{-\frac{s}{2}}E(z_0^*,s)\frac{d\varphi}{\varphi}.$$

对$1\leqslant n\leqslant M-2$, 有

$$\int_{H_n}^{H_{n+1}}d^{-\frac{s}{2}}E(z,s)\frac{d\varphi}{\varphi}=\int_{H'_{n-1}}^{H'_n}d^{-\frac{s}{2}}E(z,s)\frac{d\varphi}{\varphi}, \qquad (6.120)$$

这时φ的变化范围为

$$1<H'_{n-1}\leqslant\varphi\leqslant H'_n,$$

所以$y=\frac{\sqrt{d}}{a}\frac{\varphi}{1+\varphi^2}$的相应变化范围为

$$q_{n-1}\leqslant y^{-\frac{1}{2}}\leqslant q_n.$$

因此，这时有

$$(q_{n-1}x-p_{n-1})^2+(q_{n-1}y)^2=\left(q_{n-1}\alpha-p_{n-1}-q_{n-1}\frac{y}{\varphi}\right)^2$$

$$+(q_{n-1}y)^2<(y^{\frac{1}{2}}+y^{\frac{1}{2}})^2+(y^{\frac{1}{2}})^2=5y, \qquad (6.121)$$

这里用到下面显然的事实

$$x=\frac{\alpha'+\alpha\varphi^2}{1+\varphi^2}=\alpha-\frac{y}{\varphi};\ |q_{n-1}\alpha-p_{n-1}|<q_n^{-1},\ 若\ n\geqslant 1.$$

$E(z, s)$ 在模变换

$$z\to z^*=M<z>,\ M=\begin{pmatrix} * & * \\ q_{n-1} & -p_{n-1}\end{pmatrix}\in SL_2(\mathbb{Z}),$$

$$y^*=\frac{y}{(q_{n-1}x-p_{n-1})^2+(q_{n-1}y)^2}$$

下不变，从而由(6.121)有 $y^*\geqslant\frac{1}{5}$. 还可由

$$y^*=\frac{\sqrt{d}}{a}\cdot\frac{\varphi}{\varphi^2|q_{n-1}\alpha-p_{n-1}|^2+|q_{n-1}\alpha'-p_{n-1}|^2} \qquad (6.122)$$

再作变量替换 $\varphi\longrightarrow\varphi\delta_n^{-1}$, $\delta_n=\left|\frac{q_{n-1}\alpha-p_{n-1}}{q_{n-1}\alpha'-p_{n-1}}\right|$ 如引理中所设，则由(6.122) 即知有

$$y^*=\frac{\sqrt{d}}{a|q_{n-1}\alpha-p_{n-1}|\,|q_{n-1}\alpha'-p_{n-1}|}\cdot\frac{\varphi}{\varphi^2+1}$$

$$=\frac{\sqrt{d}}{Q_n}\,\frac{\varphi}{(1+\varphi^2)}, \qquad (6.123)$$

这里还用了 Q_n 的定义(见第一章)，新的 φ 的变化范围是

$$H_n\delta_n\leqslant\varphi\leqslant H_{n-1}\delta_n. \qquad (6.124)$$

因此由(6.120)、(6.123)和(6.124)即知

$$\int_{H_n}^{H_{n+1}}d^{-\frac{s}{2}}E(z,\ s)\frac{d\varphi}{\varphi}=\int_{H_n\delta_n}^{H_{n+1}\delta_n}d^{-\frac{s}{2}}E(z_n^*,\ s)\frac{d\varphi}{\varphi},\ 1\leqslant n\leqslant M-2,$$

$$(6.125)$$

这里

$$z_n^*=x_n^*+iy_n^*,\ y_n^*=\frac{\sqrt{d}}{Q_n}\cdot\frac{\varphi}{1+\varphi^2}\geqslant\frac{1}{5},\ x_n^*\in\mathbb{R}.$$

对 $n=M-1$，注意到 $\frac{a}{\sqrt{d}}\varepsilon^2=H_M\leqslant H'_{M-1}$，即可完全如前所述同样地得到

$$\int_{H_{M-1}}^{H_M} d^{-\frac{s}{2}}E(z,\ s)\frac{d\varphi}{\varphi}=\int_{H_{M-1}\delta_{M-1}}^{H_M\delta_{M-1}} d^{-\frac{s}{2}}E(z_{M-1}^*,\ s)\frac{d\varphi}{\varphi}, \qquad (6.126)$$

z_{M-1}^* 满足 $1\leqslant n\leqslant M-2$ 时 z_n^* 所满足的同样的性质。

总结 $k=1$，以及(6.125)与(6.126)即得

$$\frac{\Gamma\left(\frac{s}{2}\right)^2}{\Gamma(s)}\zeta_K(s)=\sum_{\mathfrak{A}=\left[a,\frac{-b+\sqrt{d}}{2}\right]}\sum_{n=0}^{M-1}\int_{H_n\delta_n}^{H_{n+1}\delta_n} d^{-\frac{s}{2}}E(z_n^*,\ s)\frac{d\varphi}{\varphi}, \qquad (6.127)$$

其中

$$z_n^*=x_n^*+iy_n^*,\ y_n^*=\frac{\sqrt{d}}{Q_n}\cdot\frac{\varphi}{1+\varphi^2}\geqslant\frac{1}{5},\ x_n^*\in\mathbb{R}.$$

由(6.127)不难得到，积分中的

$$d^{-\frac{s}{2}}E(z_j^*,\ s)=\sum_{\substack{m,n=-\infty\\(m,n)\neq(0,0)}}^{+\infty}(A_j^*m^2+B_j^*mn+C_j^*n^2)^{-s},$$

其中实数 A_j^*, B_j^*, C_j^* 满足

$$B_j^{*2}-4A_j^*C_j^*=-4d,\ A_j^*=Q_j\left(\varphi+\frac{1}{\varphi}\right)\leqslant5\sqrt{d}.$$

令 $\lambda_1<\lambda_2<\cdots$ 为正定的实系数二元二次型$((A_j^*,\ B_j^*,\ C_j^*))$所能表示的实数的全体，而 r_v 为不定方程

$$\lambda_v=A_j^*m^2+B_j^*mn+C_j^*n^2,\ m,\ n\in\mathbb{Z},\ n\neq0$$

的准确解数，易见 $\lambda_1\geqslant\frac{d}{A_j^*}$。

由引理 5.1 可得

$$d^{-\frac{s}{2}}E(z_j^*,\ s)=2\zeta(2s)(A_j^*)^{-s}+\sum_{v=1}^{\infty}r_v\lambda_v^{-s},$$

这里

$$\sum_{v=1}^{\infty}r_v\lambda_v^{-s}=s\int_{d/A_j^*}^{\infty}S(u)u^{-s-1}du=\frac{\pi}{\sqrt{d}}\frac{s}{s-1}\left(\frac{d}{A_j^*}\right)^{1-s}$$

$$+4s\int_{d/A_j^*}^{\infty}\left(\theta\sqrt{\frac{A_j^*}{4d}}-p\sqrt{\frac{1}{A_j^*}}\right)u^{-s-\frac{1}{2}}du,$$

上式的最后一个积分，当 $\sigma > \frac{1}{2}$ 时，是正则的，且其绝对值有上界

$$\frac{4|s|}{\sigma - \frac{1}{2}}\left(\frac{1}{2}\left(\frac{A_j^*}{d}\right)^\sigma + \frac{(A_j^*)^{\sigma-1}}{d^{\sigma-0.5}}\right),$$

由此即知引理已完全得证。

引理 5.3 命

$$\frac{\zeta_K(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{\nu_n}{n^s}, \quad \mathrm{Re}\, s > 1.$$

则有

$$\sum_{1<n<\frac{\sqrt{d}}{4}} \nu_n < \frac{L(1, \chi)}{2\log 2.5}\sqrt{d},$$

这里 $\chi(*) = \left(\frac{d}{*}\right)$ 是 Kronecker 符号。

证明 域 $K = Q(\sqrt{d})$ 中的每一个理想 $\mathfrak{A}$ 可以唯一地表为 $\mathfrak{A} = u\left[A, \frac{-B+\sqrt{d}}{2}\right]$，其中 u，A 为正整数，而有理整数 B 满足

$$B^2 \equiv d \pmod{4A}, \quad -A < B \leqslant A. \tag{6.128}$$

易见 $N(\mathfrak{A}) = u^2 A$，于是

$$\frac{\zeta_K(s)}{\zeta(2s)} = \sum{}^* A^{-s},$$

这里 $\sum^*$ 表示对一切满足 (6.128) 的 A，B 求和，因此有

$$\nu_n = \sum_{A=n}{}^* 1. \tag{6.129}$$

满足 (6.128) 的以 d 为判别式的有理整系数二元二次原型 $((A, B, C))$ 一定广义相似于一个约化的有理整系数二元二次原型 $((a, -b, -c))$，这里有理整数 a，b，c 满足

$$|b| \leqslant a \leqslant c, \quad d = b^2 + 4ac, \quad g.c.d.(a, b, c) = 1.$$

由第二章定理 1.3 的证明过程可知有

$$\frac{B+\sqrt{d}}{2A} \sim \frac{-b+\sqrt{d}}{2a}. \tag{6.130}$$

$\alpha = \frac{b+\sqrt{d}}{2a}$ 的简单连分数展开式为

$$\alpha=[a_0,\ \overline{a_1,\ \cdots,\ a_k}],$$

其中 $\overline{a_1,\ \cdots,\ a_k}$ 为基本周期，令 α 的第 n 个完全商为

$$\alpha_n=\frac{P_n+\sqrt{d}}{2Q_n}\quad(n\geqslant 0)$$

对满足 $A<\sqrt{d}$ 的正整数 A，存在唯一的有理整数 N，使

$$\frac{2A-B-\sqrt{d}}{2A}<\frac{-B+\sqrt{d}}{2A}<N<\frac{2A-B+\sqrt{d}}{2A},\qquad(6.131)$$

于是由(6.130)、(6.131)可知

$$\omega=\frac{P+\sqrt{d}}{2Q},\ Q=A,\ P=2AN+B\qquad(6.132)$$

满足 $\omega\in\mathfrak{M}$，$\omega\sim\dfrac{-b+\sqrt{d}}{2a}$，这里 $\mathfrak{M}$ 是第一章 1.1 小节引理 1.9 中定义的集合。因此由第一章的这个引理 1.9，即知，存在正整数 n，t 使 $1\leqslant n\leqslant k$，$1\leqslant t\leqslant a_n$，以及

$$P=2Q_{n+1}-P_{n+1}+2(P_{n+1}+Q_n)t-2Q_nt^2,\qquad(6.133)$$

$$Q=Q_{n+1}+tP_{n+1}-t^2Q_n.\qquad(6.134)$$

由(6.132)—(6.134)即有

$$\left.\begin{aligned}&A=Q_{n+1}+tP_{n+1}-t^2Q_n,\\&B=2Q_{n+1}(1-N)-P_{n+1}(1-2(1-N)t)\\&\qquad+2Q_n(1-(1-N)t)t,\\&1\leqslant n\leqslant k,\ 1\leqslant t\leqslant a_n\end{aligned}\right\}\qquad(6.135)$$

由(6.128)可知，有理整数 A，B，C 满足(已设 $A<\sqrt{d}$)

$$d=B^2-4AC,\quad |B|\leqslant A<\sqrt{d},\qquad(6.136)$$

因此由(6.132)—(6.134)可知有

$$\begin{aligned}0>C&=\frac{B^2-d}{4A}=\frac{(P-2NQ)^2-d}{4Q}\\&=\frac{(P-2Q-2(N-1)Q)^2-d}{4Q}\\&=\frac{(P-2Q)^2-d}{4Q}-(N-1)(P-2Q)+(N-1)^2Q\\&=-Q_n-(N-1)(P-2Q)+(N-1)^2Q,\end{aligned}\qquad(6.137)$$

其中用到

$$P-2Q=2tQ_n-P_{n+1},\ d=(P-2Q)^2+4QQ_n, \tag{6.138}$$

这可直接验证。于是由(6.137)与(6.138)有

$$\frac{P-2Q-\sqrt{d}}{2Q}<N-1<\frac{P-2Q+\sqrt{d}}{2Q},$$

由(6.133)、(6.134)与(6.138)即知，它即为

$$-\frac{1}{t+\dfrac{2Q_{n+1}}{\sqrt{d}+P_{n+1}}}<N-1<\frac{1}{a_n-t+\dfrac{\sqrt{d}-P_n}{2Q_n}}, \tag{6.139}$$

由(6.139)的左边的不等式即知 $N\geqslant 1$。

以下进一步假定 $A<\frac{\sqrt{d}}{4}$。我们来证明 $t=a_n$。

$N=1$ 时，用 $\frac{\sqrt{d}+B}{2A}>1$ $\left(\text{如有}\frac{\sqrt{d}+B}{2A}<1\text{，则}\sqrt{d}+B<2A<\frac{\sqrt{d}}{2}\text{，故}B<-\frac{\sqrt{d}}{2}\text{，因此}|B|>\frac{\sqrt{d}}{2}\text{这与}|B|\leqslant A<\frac{\sqrt{d}}{4}\text{矛盾}\right)$，即有

$$1<\frac{\sqrt{d}+B}{2A}=\frac{\sqrt{d}+P-2Q}{2Q}=\frac{1}{a_n-t+\dfrac{\sqrt{d}-P_n}{2Q_n}},$$

所以 $t=a_n$。

$N\geqslant 2$ 时，由(6.139)右边的不等式即得 $t=a_n$。

这样，由(6.135)可得

$$A=Q_{n-1},\ B=P_n-2(N-1)Q_{n-1},\ 1\leqslant n\leqslant k, \tag{6.140}$$

再由 $-A<B\leqslant A$，即知 N 为由下式决定的正整数

$$\frac{P_n+Q_{n-1}}{2Q_{n-1}}\leqslant N<\frac{P_n+Q_{n-1}}{2Q_{n-1}}+1, \tag{6.141}$$

当 n 给定之后，N 就唯一确定了。

$\frac{\sqrt{d}+B}{2A}(>1)$ 的简单连分数展开式如下：

$$\frac{\sqrt{d}+B}{2A}=\frac{\sqrt{d}+P_n-2(N-1)Q_{n-1}}{2Q_{n-1}}$$

$$=\frac{\sqrt{d}+2(a_{n-1}-N+1)Q_{n-1}-P_{n-1}}{2Q_{n-1}}$$

$$=[a_{n-1}-N+1,\ \overline{a_{n-2},\ \cdots,\ a_1,\ a_k,\ a_{k-1},\ \cdots,\ a_{n-2},\ a_{n-1}}]. \tag{6.142}$$

再由 $d=B^2+4A|C|$, $|B|\leqslant A<\frac{\sqrt{d}}{4}$, 可知有 $\frac{15}{4}A<|C|$。于是由第一章引理 1.3 前的(1.38), 即知应该有

$$a_{n-1}=2(a_{n-1}-N+1)+\delta,\ \delta=0,\ \pm 1,$$

即得

$$a_{n-1}=2(N-1)-\delta=2(N-1),\ 2N-1,\ 2N-3. \tag{6.143}$$

当 $N=1$ 时, 由 $a_{n-1}\geqslant 1$ 及 (6.143) 即知只可能 $a_{n-1}=1$。这时, 再用(6.142)即得

$$\frac{\sqrt{d}+P_n}{2Q_{n-1}}=\frac{\sqrt{d}+B}{2A}$$

$$=[1,\ \overline{a_{n-2},\ \cdots,\ a_k,\ a_{k-1},\ \cdots,\ a_{n-1}}]<2.$$

但这与

$$\frac{\sqrt{d}+P_n}{2Q_{n-1}}>\frac{\sqrt{d}}{2\cdot\frac{\sqrt{d}}{4}}=2$$

矛盾, 因此 $N\geqslant 2$。故由(6.141)有 $P_n>Q_{n-1}$。所以证明了

$$P_n>Q_{n-1},\ Q_{n-1}<\frac{\sqrt{d}}{4}, \tag{6.144}$$

若 n, P_n, Q_{n-1} 由(6.140)与(6.141)决定。

反之, 由满足 $1\leqslant n\leqslant k$, $Q_{n-1}<\min\left(\frac{\sqrt{d}}{4},\ P_n\right)$ 的 n, P_n, Q_{n-1}, 先由 (6.141) 决定 N, 再由 (6.140) 决定 A, B, 则理想 $\left[A,\ \frac{-B+\sqrt{d}}{2}\right]$ 满足 (6.128), 且 $A<\frac{\sqrt{d}}{4}$。

这样, 由(6.129)及上述讨论可知, 我们得到

$$\sum_{1\leqslant n<\frac{\sqrt{d}}{4}}\nu_n=\sum_{\mathfrak{A}=\left[a,\ \frac{-b+\sqrt{d}}{2}\right]}\ \sum_{\substack{j=0\\ Q_j<\min\left(\frac{\sqrt{d}}{4},\ P_{j+1}\right)}}^{k-1}1, \tag{6.145}$$

这里 $\mathfrak{A}=\left[a,\ \frac{-b+\sqrt{d}}{2}\right]$跑过 $K=Q(\sqrt{d})$ 的理想类群 $\mathscr{C}_K$ 的一个完全代表之组，它们满足条件：

$$|b|\leqslant a\leqslant c,\ d=b^2+4ac,\ a,\ b,\ c\in\mathbf{Z},\ g.c.d.(a,\ b,\ c)=1;$$

$\alpha=\frac{b+\sqrt{d}}{2a}$具有上述所列的简单连分数展开式及完全商。

由 $Q_k=Q_0$ 及 K 的基本单位（见第一章、第二章有关结果）

$$\varepsilon=\prod_{j=1}^{k}\frac{\sqrt{d}+P_j}{2Q_j}=\prod_{j=1}^{k}\frac{\sqrt{d}+P_j}{2Q_{j-1}}>\prod_{\substack{j=1\\ Q_{j-1}<\min\left(P_j,\frac{\sqrt{d}}{4}\right)}}^{k}\frac{\sqrt{d}+P_j}{2Q_{j-1}},$$

可得

$$\log\varepsilon>\log(2.5)\sum_{\substack{j=1\\ Q_{j-1}<\min\left(P_j,\frac{\sqrt{d}}{4}\right)}}^{k}1,\tag{6.146}$$

因为

$$\frac{\sqrt{d}+P_j}{2Q_{j-1}}>2.5,\ 如\ Q_{j-1}<\min\left(P_j,\ \frac{\sqrt{d}}{4}\right).$$

这样，由(6.145)与(6.146)即得

$$\sum_{1<n<\frac{\sqrt{d}}{4}}\nu_n<\frac{h\log\varepsilon}{\log 2.5}=\frac{\sqrt{d}\,L(1,\ \chi)}{2\log 2.5},$$

这里 h 是 $K=Q(\sqrt{d})$ 的类数，最后一步用到类数公式，因此引理得证。

引理 5.4　对 $0<10y<x,\ 0<\delta<\frac{1}{10}$，有

$$\sum_{y<n<x}\nu_n n^{-\frac{1}{2}}<L(1,\ \chi)\left(5.26\sqrt{d}\,y^{-\frac{1}{2}}+302\sqrt{x}\right.$$
$$\left.+28\delta^{-1}x^{\frac{1}{2}-\delta}d^{\delta}\right).$$

证明　对 $c>0$，令

$$K(c)=\int_0^{\infty}\exp\left(-c\left(u+\frac{1}{u}\right)\right)\frac{du}{u},\tag{6.147}$$

则由 Mellin 变换（见参考文献[86]）有

$$2K\left(\frac{1}{x}\right)=\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}x^s\Gamma^2\left(\frac{s}{2}\right)ds,\ 如\ x>0.\tag{6.148}$$

对 $y\leqslant n\leqslant x$ 与 $0<10y<x$，有

$$\exp\left(-\frac{n}{x}\left(u+\frac{1}{u}\right)\right)-\exp\left(-\frac{n}{y}\left(u+\frac{1}{u}\right)\right)\geqslant\exp\left(-\left(u+\frac{1}{u}\right)\right)$$

$$\cdot\left(1-\exp\left(-\frac{9}{10}\cdot\frac{n}{y}\left(u+\frac{1}{u}\right)\right)\right)>0.8347\exp\left(-\left(u+\frac{1}{u}\right)\right),$$

于是由 (6.147) 有

$$2K\left(\frac{n}{x}\right)-2K\left(\frac{n}{y}\right)>3.3388\int_1^{\infty}\exp\left(-\left(u+\frac{1}{u}\right)\right)\frac{du}{u}>\frac{1}{2.63},\tag{6.149}$$

这里用到

$$\int_1^{\infty}\exp\left(-u-\frac{1}{u}\right)\frac{du}{u}=K_0(2)$$
$$=\sum_{l=0}^{\infty}\frac{1}{(l!)^2}\left(\sum_{j=1}^{l}\frac{1}{j}-\gamma\right)>0.113893$$

其中 $\gamma=0.57721566490\cdots$ 是 Euler 常数，$K_0(X)$ 是 Bessel 函数。由 (6.148) 与 (6.149) 可得

$$\sum_{y<n<x}\nu_n<\frac{2.63}{2\pi i}\int_{2-i\infty}^{2+i\infty}\Gamma^2\left(\frac{s}{2}\right)\frac{\zeta_K(s)}{\zeta(2s)}(x^s-y^s)ds,\tag{6.150}$$

把引理 5.2 用到这里，再对所涉及的积分分别计算如下：

$$2\sum_{\mathfrak{A}}\sum_{n=0}^{M-1}\int_{H_n\delta_n}^{H_{n+1}\delta_n}\left(\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}(A_n^*)^{-s}\Gamma(s)(x^s-y^s)ds\right)\frac{d\varphi}{\varphi}$$
$$=2\sum_{\mathfrak{A}}\sum_{n=0}^{M-1}\int_{H_n\delta_n}^{H_{n+1}\delta_n}\left(\exp\left(-\frac{A_n^*}{x}\right)-\exp\left(-\frac{A_n^*}{y}\right)\right)\frac{d\varphi}{\varphi}$$
$$<2\sum_{\mathfrak{A}}\log\varepsilon^2=4h\log\varepsilon=2L(1,\ \chi)\sqrt{d},\tag{6.151}$$

其中用到

$$\sum_{n=0}^{M-1}\int_{H_n\delta_n}^{H_{n+1}\delta_n}\frac{d\varphi}{\varphi}=\sum_{n=0}^{M-1}\int_{H_n}^{H_{n+1}}\frac{d\varphi}{\varphi}=2\log\varepsilon,$$

以及类数公式：

$$\left|\frac{\pi}{\sqrt{d}}\sum_{\mathfrak{A}}\sum_{n=0}^{M-1}\int_{H_n\delta_n}^{H_{n+1}\delta_n}\right.$$
$$\left.\left(\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{s}{1-s}\left(\frac{d}{A_n^*}\right)^{1-s}\frac{\Gamma(s)}{\zeta(2s)}(x^s-y^s)ds\right)\frac{d\varphi}{\varphi}\right|$$
$$\leqslant\frac{\pi L(1,\ \chi)(x-y)}{\zeta(2)}+\frac{1+10^{-1+\delta}}{2\delta}\cdot\frac{\zeta(2-2\delta)}{\zeta(4-4\delta)}L(1,\ \chi)$$

$$\cdot x^{1-\delta}d^{\delta}\int_{-\infty}^{+\infty}|\Gamma(1-\delta+\mathrm{i}t)|\,dt$$

$$<\frac{6}{\pi}L(1,\ \chi)x+4.7\delta^{-1}L(1,\ \chi)x^{1-\delta}d^{\delta},\qquad(6.152)$$

其中的过程如下：首先把积分限移到 $\mathrm{Re}s=1-\delta\left(0<\delta<\frac{1}{10}\right)$ 处，并注意到在 $s=1-\delta+\mathrm{i}t$ 处，有

$$\left|\frac{s}{1-s}(A_n^*)^{s-1}\right|=\left|\frac{1-\delta+\mathrm{i}t}{\delta-\mathrm{i}t}\right|\left(Q_n\left(\varphi+\frac{1}{\varphi}\right)\right)^{-\delta}$$

$$\leqslant\left(\frac{(1-\delta)^2+t^2}{\delta^2+t^2}4^{-\delta}\right)^{\frac{1}{2}}\leqslant\frac{\sqrt{1-\delta^2}}{\delta}2^{-\delta},$$

$$\int_{-\infty}^{+\infty}|\Gamma(1-\delta+\mathrm{i}t)|\,dt=\int_{-\infty}^{+\infty}\left|\frac{\Gamma(3-\delta+\mathrm{i}t)}{(1-\delta+\mathrm{i}t)(2-\delta+\mathrm{i}t)}\right|dt$$

$$\leqslant\Gamma(3-\delta)\int_{-\infty}^{+\infty}\frac{dt}{\sqrt{((1-\delta)^2+t^2)((2-\delta)^2+t^2)}}$$

$$\leqslant1.113\pi\sqrt{\frac{1.9}{0.9}}.$$

$$\frac{\zeta(2-2\delta)}{\zeta(4-4\delta)}<\frac{\zeta\left(\frac{9}{5}\right)}{\zeta(4)}<171\pi^{-4},$$

即可得出(6.152)。

最后有

$$\left|\frac{1}{2\pi\mathrm{i}}\int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty}R_1(s)\Gamma(s)(x^s-y^s)\frac{ds}{\zeta(2s)}\right|$$

$$\leqslant\frac{4}{\pi}\cdot\frac{\zeta(2)}{\zeta(4)}\left(\frac{5}{2}+1\right)\left(1+\frac{1}{10}\right)L(1,\ \chi)$$

$$\cdot x\int_{-\infty}^{+\infty}|\Gamma(1+\mathrm{i}t)|\sqrt{1+t^2}\,dt<57.4L(1,\ \chi)x.$$

$$(6.153)$$

这里的过程如下：先把积分路径移到 $\mathrm{Re}s=1$ 处，再利用 $R_1(s)$ 的估计式(引理 5.2) 和 $A_n^*<5\sqrt{d}$，以及

$$\int_{-\infty}^{+\infty}|\Gamma(1+\mathrm{i}t)|\sqrt{1+t^2}\,dt$$

$$=\int_{-\infty}^{+\infty}\left|\frac{\Gamma(4+\mathrm{i}t)}{(2+\mathrm{i}t)(3+\mathrm{i}t)}\right|dt\leqslant\sqrt{6}\,\pi.$$

综合(6.151)、(6.152)和(6.153)，并用 (6.150) 与引理 5.2 即得

$$S(y,\ x)\overset{\text{def}}{=}\sum_{x<n<y}\nu_n<2.63L(1,\ \chi)(2\sqrt{d}+57.4x+4.7\delta^{-1}x^{1-\delta}d^{\delta}),$$

从而可得

$$\sum_{y<n<x}\nu_n n^{-\frac{1}{2}}\leqslant x^{-\frac{1}{2}}S(y,\ x)+\frac{1}{2}\int_y^x S\left(\frac{y}{10},\ u\right)u^{-\frac{3}{2}}du$$

$$<L(1,\ \chi)(5.26\sqrt{d}\,y^{-\frac{1}{2}}+302\sqrt{x}+28\delta^{-1}x^{\frac{1}{2}-\delta}d^{\delta}),$$

即得引理。

引理 5.5 设 $\frac{1}{4}\sqrt{d}<d<x$，$10<y<\frac{1}{4}\sqrt{d}$，则有

$$\sum_{y<n<x}n^{-\frac{1}{2}}\sum_{1<m|n}\nu_m\nu_{\frac{n}{m}}\leqslant 11276(L(1,\ \chi)^2xy^{-\frac{1}{2}}+L(1,\ \chi)x^{\frac{1}{2}})(\log y)^3.$$

证明 对 $y\leqslant\sqrt{x}$，有

$$\sum_{y<n<x}n^{-\frac{1}{2}}\sum_{1<m|n}\nu_m\nu_{\frac{n}{m}}\leqslant\left(\sum_{y<n<\frac{x}{y}}\nu_n n^{-\frac{1}{2}}\right)^2+2\sum_{y<n<x}n^{-\frac{1}{2}}\sum_{\substack{1<m|n\\1<m<y}}\nu_m\nu_{\frac{n}{m}},\tag{6.154}$$

由引理 5.3 与引理 5.4，以及下述的

$$\sum_{1<m<y}\frac{\nu_m}{m}\leqslant\sum_{1<m<y}\frac{1}{m}\sum_{1<n|m}1\leqslant\sum_{1<n<y}\frac{1}{n}\left(1+\int_1^{\frac{y}{n}}\frac{du}{u}\right)<(1+\log y)^2$$

可知，对任意的 $0<\delta<0.1$，有

$$\left(\sum_{y<n<\frac{x}{y}}\nu_n n^{-\frac{1}{2}}\right)^2<L(1,\ \chi)^2y^{-1}\left(307.26\sqrt{x}+28\sqrt{x}\frac{y^{\delta}}{\delta}\right)^2\tag{6.155}$$

和

$$\sum_{y<n<x}n^{-\frac{1}{2}}\sum_{\substack{1<m|n\\1<m<y}}\nu_m\nu_{\frac{n}{m}}=\sum_{1<m<y}\nu_m m^{-\frac{1}{2}}\sum_{\frac{y}{m}<n<\frac{x}{m}}\nu_n n^{-\frac{1}{2}}$$

$$<L(1,\ \chi)\sum_{1<m<y}\nu_m m^{-\frac{1}{2}}\left(5.26\sqrt{d}\left(\frac{m}{y}\right)^{\frac{1}{2}}+302\left(\frac{x}{m}\right)^{\frac{1}{2}}\right.$$

$$+\frac{28}{\delta}\left(\frac{x}{m}\right)^{\frac{1}{2}-\delta}d^{\delta}\Big)<\frac{5.26}{2\log 2.5}L(1,\ \chi)^{2}dy^{-\frac{1}{2}}$$

$$+L(1,\ \chi)x^{\frac{1}{2}}(1+\log y)^{2}\left(302+\frac{28}{\delta}y^{\delta}\right),\qquad(6.156)$$

取

$$\delta=\frac{\log 10}{10\log y}<\frac{1}{10},\ 如\ y>10,$$

则由(6.154)～(6.156)即得引理。

引理 5.6　设 $10y<x<d,\ 10<y<\min\left(\frac{\sqrt{d}}{4},\ \frac{x}{10}\right)$，则有

$$\sum_{y<n<x}n^{-\frac{1}{2}}\sum_{1<m|n}\nu_m\nu_{\frac{n}{m}}\ll(L(1,\chi)^{2}y^{-\frac{1}{2}}+L(1,\ \chi)x^{\frac{2}{5}}d^{0.1})(\log y)^{3},$$

这里“≪”所含的正常数是可以有效计算的绝对常数。

证明　与引理 5.5 的证明类似，只要注意到在本引理的条件下，有

$$x^{\frac{1}{2}}<x^{\frac{1}{2}-\delta}d^{\delta}<x^{0.4}d^{0.1}<d^{0.5},\ 若\ 0<\delta<0.1,$$

即可得引理。

引理 5.7　设 N_0 为一个给定的正整数，再设 $d>\exp(500N_0^3)$，那么当 $L(1,\ \chi)<\frac{(\log d)^{N_0}}{\sqrt{d}}$ 时，有

$$|\{p\ 有理素数|\ p<(\log d)^{N_0},\ \chi(p)\neq-1\}|\leqslant 2N_0\log\log d$$

以及

$$\mathrm{P}\stackrel{\mathrm{def}}{=\!=}\prod_{\substack{\chi(p)\neq-1\\ p<(\log d)^{N_0}}}(1+p^{-\frac{1}{2}})<\exp(5\sqrt{N_0\log\log d}),$$

这里 p 跑过有理素数，$\chi(*)=\left(\frac{d}{*}\right)$是 Kronecker 符号。

证明　记

$$\mathscr{P}=\{p\ 有理素数|\ p<(\log d)^{N_0},\ \chi(p)\neq-1\}.$$

我们先来证明 $\mathscr{P}$ 的元素个数 $|\mathscr{P}|\leqslant 2N_0\log\log d$.

命 m 为小于等于$\left(\log\frac{\sqrt{d}}{4}\right)(N_0\log\log d)^{-1}$的最小正整数，易见

$$m \geqslant 40,\ m > \frac{\log \frac{\sqrt{d}}{4}}{N_0 \log\log d} - 1. \tag{6.157}$$

首先证明 $|\mathscr{P}|<m$。如有 $|\mathscr{P}|\geqslant m$，则 $\mathscr{P}$ 中至少有 m 个素数 $p_1, \cdots, p_m$，它们满足 $p_j<(\log d)^{N_0}$，$\chi(p_j)\neq -1$，$1\leqslant j\leqslant m$。任取其中的 u 个：$p_{j_1}, \cdots, p_{j_u}$；再任取 u 个正整数 $l_1, \cdots, l_u$，使 $l_1+\cdots+l_u\leqslant m$。则有

$$n \overset{\text{def}}{=\!=} p_{j_1}^{l_1}\cdots p_{j_u}^{l_u} < (\log d)^{mN_0} \leqslant \frac{\sqrt{d}}{4},$$

于是 $\nu_n\geqslant 1$，从而有

$$\sum_{1<n<\frac{\sqrt{d}}{4}} \nu_n \geqslant 1 + \sum_{u=1}^{m}\binom{m}{u}\sum_{\substack{l_1+\cdots+l_u<m\\ l_1,\cdots,l_u\geqslant 1}} 1$$

$$= 1 + \sum_{u=1}^{m}\binom{m}{u}^2 = \binom{2m}{m} \geqslant \frac{4^m}{2m} > 3^m,$$

因此由引理 5.2 可知

$$m < \frac{1}{\log 3}\log\left(\frac{\sqrt{d}\,L(1,\chi)}{2\log 2.5}\right) < N_0\log\log d,$$

这与(6.157)矛盾。

这就证明了我们有 $|\mathscr{P}|<m$。对 $\mathscr{P}$ 中的任意 l 个素数 $p_1, \cdots, p_l$，有

$$n \overset{\text{def}}{=\!=} p_1\cdots p_l < (\log d)^{lN} < (\log d)^{mN_0} \leqslant \frac{\sqrt{d}}{4},$$

于是 $\nu_n\geqslant 1$，从而有

$$\sum_{1<n<\frac{\sqrt{d}}{4}} \nu_n \geqslant 1 + \sum_{l=1}^{|\mathscr{P}|}\binom{|\mathscr{P}|}{l} = 2^{|\mathscr{P}|},$$

由此及引理 5.2 即得

$$|\mathscr{P}| \leqslant 2N_0\log\log d.$$

所以

$$\log P = \sum_{p\in\mathscr{P}}\log(1+p^{-\frac{1}{2}}) < \sum_{p\in\mathscr{P}} p^{-\frac{1}{2}} \leqslant \frac{5\sqrt{2}}{2}|\mathscr{P}|^{\frac{1}{2}}$$

$$\leqslant 5\sqrt{N_0\log\log d},$$

这里用到：对任一个素数集合 $\mathscr{P}$，均有

$$\sum_{p\in\mathscr{P}} p^{-\frac{1}{2}}\leqslant\frac{5}{2}\sqrt{2}\,|\mathscr{P}|^{\frac{1}{2}},$$

这是不难证明的。

引理证毕。

5.2 Goldfeld 定理的讨论

本章的后面部分致力于下述定理的证明。

定理 5.1(D. Goldfeld[22]) 设 $K=Q(\sqrt{d})$ 是一个判别式为 d 的实二次域。假定存在一条 Weil 椭圆曲线 E，它的秩与导子分别为 g 与 N，满足弱 BSD 猜想，即它的 L 函数 $L_E(s)$ 在 $s=1$ 处有一个 g 阶零点。再设 $g.c.d.(d, N)=1$。令 $\mu=1, 2$ 由 $\chi(-N)=(-1)^{g-\mu}$ 所决定，这里 $\chi(*)=\left(\frac{d}{*}\right)$ 为 Kronecker 符号。那么存在两个可以有效地计算的绝对正常数 c_1, c_2，它们与 g、N、d 均无关，使得，当 $d>\exp\exp(c_1Ng^3)$ 时，有

$$L(1, \chi)>\frac{c_2}{g^{4g}N^3}\cdot\frac{(\log d)^{g-\mu-1}\exp(-21\sqrt{g\log\log d})}{\sqrt{d}}.$$

附注 (1) Goldfeld 定理对虚二次域也成立，只需把 d 换为域判别式的绝对值。由于对虚二次域具有上述性质的 $g\geqslant 3$ 的椭圆曲线已经具体找到，因而有了更精密的 GGZO 定理(见第 5 章)，所以我们在此只讨论实二次域的情况。

(2) 由定理 5.1 的结论可见，要使它真正有效，g 至少大于等于 4。但现在对找到这种性质的椭圆曲线还无能为力，所以定理 5.1 还不能发挥实际的作用。

(3) 在 $g.c.d.(d, N)>1$ 的情况下，定理 5.1 仍然成立，只是条件 $\chi(-N)=(-1)^{g-\mu}$ 将由更为复杂的条件所替代，这可参考第五章的有关的叙述以及有关的参考文献，为了证明的简便起见，不再叙述了。

定理 5.1 的证明，基本上采用 D. Goldfeld 的原始证明，这是为了与 GGZO 定理的证明加以比较。

我们要来证明比定理 5.1 更强些的下列的定理 5.2。

定理 5 2　在定理 1 的条件下，我们有

$$L(1,\ \chi) \gg \frac{g^{-4g} N^{-3} (\log d)^{g-\mu-1}}{\sqrt{d}\,(\log\log d)^{g-\mu+4}} \prod_{\substack{\chi(p) \neq -1 \\ p < (\log d)^{8g}}} \left(1 + p^{-\frac{1}{2}}\right)^{-4},$$

这里 p 表有理素数，“$\gg$”所含正常数是一个与 g、N、d 均无关的可以有效地计算的绝对正常数。

附注　(4) 对素数 $d = 4n^2 + 1$（n 为正整数），如 $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ 的类数为 1，则已知对小于 n 的素数 p 均有 $\chi(p) = -1$。所以对充分大的 d（只要满足定理 5.1 的条件），定理 5.2 结论中的右边乘积为 1。因此只要假定存在一条 Weil 椭圆曲线 E，其秩 g 为 4，其导子为一个素数 N，并且它还满足弱 BSD 猜想，即其 L 函数 $L_E(s)$ 在 $s = 1$ 处有一个 4 阶零点，则当 d 充分大时（这个界只依赖于 g、N 且可有效地计算），$\mu = 1$，

$$L(1,\ \chi) \gg \frac{N^{-3} (\log d)^{2}}{\sqrt{d}\,(\log\log d)^{7}},$$

这里“$\gg$”所含的正常数与 g、N、d 均无关，且是可以有效地计算的绝对正常数。这样用类数公式

$$2h \log \varepsilon = \sqrt{d}\, L(1,\ \chi), \quad \varepsilon = 2n + \sqrt{d},$$

即可得出

$$\frac{\log d}{(\log\log d)^{7}} \ll N^{3},$$

“$\ll$”所含正常数是可以有效地计算的绝对正常数，因此存在一个绝对正常数 c 使

$$d < \exp(N^{c}),$$

所以结合 §4 的结果，即知 S. Chowla 猜想可以由此基本上解决。

5.3　Goldfeld 定理的证明(一)

Goldfeld 定理的证明与 GGZO 定理的证明实质上是相同的，所以我们往往用第五章的有关结果而不一一加以说明，因此请读者参考那里的有关内容。

对所给的 Weil 曲线 E，它的 L 函数

$$L_E(s)=\sum_{n=1}^{\infty}a_n n^{-s}=\prod_{p\mid N}(1-a_p p^{-s})^{-1}$$

$$\prod_{p\nmid N}(1-\alpha_p p^{\frac{1}{2}-s})^{-1}(1-\bar{\alpha}_p p^{\frac{1}{2}-s})^{-1},\ \mathrm{Re}s>\frac{1}{2},\tag{6.158}$$

其中 a_n 为有理整数，并有 $a_1=1$，以及

$$\left.\begin{array}{l}a_p=0,\ 如\ p^2\mid N;\ a_p=\pm1,\ 如\ p\| N;\\ |\alpha_p|=1,\ 如\ p\nmid N;\ |a_n|\leqslant\sqrt{n}\,\tau(n),\ n\in N;\end{array}\right\}\tag{6.159}$$

其中 $\tau(n)$ 是 n 的正因子的个数。

$L_E(s)$ 的 χ-twist

$$L_E(s,\ \chi)=\sum_{n=1}^{\infty}a_n\chi(n)n^{-s},\ \mathrm{Re}s>\frac{3}{2}.\tag{6.160}$$

$$\xi_E(s)\overset{\mathrm{def}}{=\!=}N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L_E(s)\ 与\ \xi_E(s,\ \chi)$$

$$\overset{\mathrm{def}}{=\!=}(d^2N)^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L_E(s,\ \chi),\tag{6.161}$$

均可解析开拓为 s 的整函数，且满足函数方程

$$\xi_E(s)=w_E\xi_E(2-s),\ w_E=\pm1,\tag{6.162}$$

$$\xi_E(s,\ \chi)=w_{E,\chi}\xi_E(2-s,\ \chi),\ w_{E,\chi}=\chi(-N)w_E.\tag{6.163}$$

注意，我们已设 $g.c.d.(d,\ N)=1$。令 $\lambda(n)$ 为 Liouville 函数，即 $\lambda(n)=\prod_{p^\alpha\| n}(-1)^\alpha$。置

$$\tilde{L}(s)=L_E\left(\frac{s}{2}\right)L_E\left(\frac{s}{2},\ \lambda\right)\prod_{p\nmid N}(1-p^{1-s})^{-1},\tag{6.164}$$

其中

$$L_E(s,\ \lambda)=\sum_{n=1}^{\infty}a_n\lambda(n)n^{-s},\ \mathrm{Re}s>\frac{3}{2},\tag{6.165}$$

则

$$\tilde{L}(s)=\prod_{p\nmid N}(1+p^{1-s})^{-1}\sum_{n=1}^{\infty}a_n^2n^{-s},\ \mathrm{Re}s>2,\tag{6.166}$$

并且函数

$$\tilde{\Lambda}(s)\overset{\mathrm{def}}{=\!=}N^s(2\pi)^{-s}\Gamma(s)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\tilde{L}(s)\tag{6.167}$$

可以解析开拓为 s 的整函数，同时满足函数方程

$$\tilde{\Lambda}(3-s)=\tilde{\Lambda}(s),\tag{6.168}$$

还有

$$\tilde{\Lambda}(2)=N\iint\limits_{D_0(N)}|f(\tau)|^2|d\tau\Lambda d\bar{\tau}|>0, \tag{6.169}$$

这里

$$f(\tau)=\sum^{\infty}a_nq^n\,(q=e^{2\pi i\tau},\ \mathrm{Im}\tau>0) \tag{6.170}$$

是群 $\Gamma_0(N)$ 的权为 2 的尖点形式，$D_0(N)$ 是上半平面 H 在

$$\Gamma_0(N)=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})\,\middle|\, c\equiv 0\,(\mathrm{mod}N)\right\}$$

下的基域。注意 $f(\tau)$ 的 Fourier 系数与 L 级数 $L_E(s)$ 的系数是相同的，这些 a_n 满足 (6.159)，a_n 全是有理整数，且 $a_1=1$。

令 $\tau=x+iy$，x，$y\in\boldsymbol{R}$。则由 (6.169) 有

$$\tilde{\Lambda}(2)=N\iint\limits_{D_0(N)}|f(\tau)|^2\frac{dxdy}{y^2}\geqslant N\iint\limits_{D_0(1)}|f(\tau)|^2\frac{dxdy}{y^2}, \tag{6.171}$$

这里 $D_0(1)$ 是上半平面 H 在 $\Gamma_0(1)$ 下的基域。

$$\begin{aligned} D_0(1)&=\left\{x+iy\in H\,\middle|\,-\frac{1}{2}\leqslant x<\frac{1}{2},\ x^2+y^2>1\right\}\\ &\quad\cup\left\{e^{i\varphi}\,\middle|\,\frac{\pi}{2}\leqslant\varphi<\frac{2\pi}{3}\right\}\\ &\supset\left\{x+iy\in H\,\middle|\,-\frac{1}{2}\leqslant x<\frac{1}{2},\ y\geqslant 1\right\}. \end{aligned}$$

因此，由 (6.171) 即得

$$\begin{aligned} \tilde{\Lambda}(2)&\geqslant N\int_1^{\infty}\left(\int_{-\frac{1}{2}}^{\frac{1}{2}}|f(\tau)|^2dx\right)\frac{dy}{y}\\ &=N\sum_{m,n=1}^{\infty}a_ma_n\int_{-\frac{1}{2}}^{\frac{1}{2}}e^{2\pi i(m-n)x}dx. \end{aligned}$$

$$\begin{aligned} &\int_1^{\infty}e^{-2\pi(m+n)y}\frac{dy}{y^2}=N\sum^{\infty}a_n^2\int_1^{\infty}e^{-4\pi ny}\frac{dy}{y^2}\\ &\geqslant N\int_1^{\infty}e^{-4\pi y}\frac{dy}{y^2}>\frac{N}{4}\int_1^2e^{-4\pi y}dy=\frac{e^{-4\pi}-e^{-8\pi}}{16\pi}N, \end{aligned}$$

故得

$$\tilde{A}(2)>6\times10^{-8}N. \tag{6.172}$$

命

$$\Psi(s)=L_E(s)L_E(s,\lambda),\ G(s)=L_E(s,\chi)L_E(s,\lambda)^{-1} \tag{6.173}$$

则由定义与(6.159)，不难证明

$$\Psi(s)\lll\zeta(2s-1)^2,\ G(s)\lll\left(\frac{\zeta_K\left(s-\frac{1}{2}\right)}{\zeta(2s-1)}\right)^2 \tag{6.174}$$

这里"$\lll$"的定义与上述事实的证明，见第五章。

由(6.173)与(6.174)可得

$$\varphi(s)\overset{\text{def}}{=\!=}L_E\left(s+\frac{1}{2}\right)L_E\left(s+\frac{1}{2},\chi\right)\lll(\zeta(2s))^2\left(\frac{\zeta_K(s)}{\zeta(2s)}\right)^2, \tag{6.175}$$

记

$$\varphi(s)=\sum_{n=1}^{\infty}b_n n^{-s},\ \mathrm{Re}\ s>1, \tag{6.176}$$

则由定义及(6.175)有

$$|b_n|\leqslant\sum_{\substack{n_1n_2m^2=n\\ n_1,n_2,m\geqslant1}}\tau(m)\nu_{n_1}\nu_{n_2}, \tag{6.177}$$

注意

$$\frac{\zeta_K(s)}{\zeta(2s)}=\sum_{n=1}^{\infty}\frac{\nu_n}{n^s},\ \mathrm{Re}\ s>1,$$

$\tau(n)$是n的正因子的个数。

命

$$F(s)=\xi_E(s)\xi_E(s,\chi)=M^s\Gamma(s)^2L_E(s)L_E(s,\chi),$$
$$M=\frac{dN}{4\pi^2}, \tag{6.178}$$

$F(s)$ 是 s 的一个整函数，且满足函数方程

$$F(2-s)=\chi(-N)F(s), \tag{6.179}$$

这些事实是(6.161)—(6.163)的推论。

令 $k=g-\mu$。则有$1+\chi(-N)(-1)^{g-\mu}=2$，这里g是E的秩，且也是$L_E(s)$在$s=1$处零点的阶，这是因为我们已假定E满

足弱BSD猜想. 进一步假定 k 大于等于3, 这是因为我们有显然估计

$$\sqrt{d}\,L(1,\ \chi)>\frac{2}{3}\log d.$$

设 $s=\sigma+\mathrm{i}t,\ 0<\mathrm{Re}\,s=\sigma<1$.

由函数方程(6.179)可知积分

$$\begin{aligned}
&\frac{1}{2\pi\mathrm{i}}\int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty}F\left(\frac{3}{2}-s+z\right)\frac{dz}{z}\\
&=\frac{\chi(-N)}{2\pi\mathrm{i}}\int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty}F\left(\frac{1}{2}+s-z\right)\frac{dz}{z}\\
&=\chi(-N)\,F\left(\frac{1}{2}+s\right)+\frac{\chi(-N)}{2\pi\mathrm{i}}\int_{-2-\mathrm{i}\infty}^{-2+\mathrm{i}\infty}F\left(\frac{1}{2}+s-z\right)\frac{dz}{z}\\
&=\chi(-N)F\left(\frac{1}{2}+s\right)-\frac{\chi(-N)}{2\pi\mathrm{i}}\int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty}F\left(\frac{1}{2}+s+z\right)\frac{dz}{z},
\end{aligned}\tag{6.180}$$

这里对 $F(s)$ 的阶的估计是为移动积分路径所必须的, 这可同第五章一样得到, 在此我们不再赘述了. 由(6.180)可得

$$\begin{aligned}
F\left(\frac{1}{2}+s\right)=&\frac{1}{2\pi\mathrm{i}}\int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty}F\left(\frac{1}{2}+s+z\right)\frac{dz}{z}\\
&-\frac{\chi(-N)}{2\pi\mathrm{i}}\int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty}F\left(\frac{3}{2}-s+z\right)\frac{dz}{z},
\end{aligned}$$

再用(6.178)、(6.175)与(6.176)即得

$$\begin{aligned}
F\left(\frac{1}{2}+s\right)=&\sqrt{M}\sum_{n=1}^{\infty}b_n\left(\frac{M}{n}\right)^s\frac{1}{2\pi\mathrm{i}}\\
&\cdot\int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty}\Gamma\left(\frac{1}{2}+s+z\right)^2\left(\frac{M}{n}\right)^z\frac{dz}{z}\\
&+\chi(-N)\sqrt{M}\sum_{n=1}^{\infty}b_n\left(\frac{M}{n}\right)^{1-s}\frac{1}{2\pi\mathrm{i}}\\
&\cdot\int_{2-\mathrm{i}\infty}^{2+\mathrm{i}\infty}\Gamma\left(\frac{3}{2}-s+z\right)^2\left(\frac{M}{n}\right)^z\frac{dz}{z},
\end{aligned}$$

由 Mellin 变换, 即得

$$F\left(\frac{1}{2}+s\right)=M\sum_{n=1}^{\infty}\frac{b_n}{\sqrt{n}}\int_{u_1=0}^{\infty}\int_{u_2=\frac{n}{Mu_1}}^{\infty}$$

$$\left[\left(\frac{Mu_1u_2}{n}\right)^{s-\frac{1}{2}}+\chi(-N)\left(\frac{Mu_1u_2}{n}\right)^{\frac{1}{2}-s}\right]e^{-u_1-u_2}du\,du_2,$$

由此即知

$$\frac{d^k}{ds^k}F\left(\frac{1}{2}+s\right)\bigg|_{s=\frac{1}{2}}=2M\sum_{n=1}^{\infty}\frac{b_n}{\sqrt{n}}\int_{u_1=0}^{\infty}\int_{u_2=\frac{n}{Mu_1}}^{\infty}\left(\log\frac{Mu_1u_2}{n}\right)^k e^{-u_1-u_2}du_1du_2. \quad (6.181)$$

由 $F(s)$ 的定义 (6.178) 即知它在 $s=1$ 处有一个阶大于等于 g 的零点。又 $3\leqslant k=g-\mu\leqslant g-1$，所以 (6.181) 的左边为 0。因此有

$$0=\sqrt{M}\sum_{n=1}^{\infty}\frac{b_n}{\sqrt{n}}\int_{u_1=0}^{\infty}\int_{u_2=\frac{n}{Mu_1}}^{\infty}\left(\log\frac{Mu_1u_2}{n}\right)^k e^{-u_1-u_2}du_1du_2$$

$$=\sum_{v=0}^{k}\binom{k}{v}\sum_{n=1}^{\infty}b_n\sqrt{\frac{M}{n}}\left(\log\frac{M}{n}\right)^{k-v}I_v\left(\frac{n}{M}\right), \quad (6.182)$$

其中，对 $x>0$，有

$$I_v(x)=\int_{u_1=0}^{\infty}\int_{u_2=\frac{x}{u_1}}^{\infty}(\log(u_1u_2))^v e^{-u_1-u_2}du_1u_2. \quad (6.183)$$

不难证明下列的估计：

$$|I_v(x)|\leqslant\begin{cases}2^{v+1}v!\,, & \text{如 } x\geqslant 0;\\ 2^{v+1}(v+1)!\,(\log x)^v e^{-\sqrt{x}}, & \text{如 } x\geqslant 3.\end{cases} \quad (6.184)$$

把 (6.182) 的右边分为两项：

$$0=\sum_{u=0}^{k}\binom{k}{v}\left(\sum_{n<A}+\sum_{n>A}\right)=\Sigma_1+\Sigma_2, \quad (6.185)$$

其中

$$A=M((8+2k)\log M)^2. \quad (6.186)$$

则有

$$\Sigma_1=-\Sigma_2. \quad (6.187)$$

5.4 Goldfeld 定理的证明(二)

引理 5.8 设 $d>\exp(500g^3)$，则有

$$|\Sigma_2|\leqslant 1.$$

证明 由 (6.175) 可知 $\varphi(s)\ll(\zeta(s))^4$，故有 $|b_n|\leqslant 3\sqrt{3}n$.

这样(注意 $k\geqslant 3$)由(6.182)~(6.186)可得

$$|\Sigma_2|\leqslant 3\sqrt{3}M\sum_{v=0}^{k}\binom{k}{v}\sum_{n>A}\sqrt{n}\left(\log\frac{n}{M}\right)^{k-v}\left|I_v\left(\frac{n}{M}\right)\right|$$

$$\leqslant 3\sqrt{3}M\sum_{v=0}^{k}(v+1)!\binom{k}{v}2^{v+1}\sum_{n>A}\sqrt{\frac{n}{M}}\left(\log\frac{n}{M}\right)^{k}e^{-\sqrt{\frac{n}{M}}}$$

$$\leqslant 3\sqrt{3}M(k+1)!\,2^{k+2}\int_{\frac{A}{4M}}^{\infty}\sqrt{u}\,(\log u)^{k}e^{-\sqrt{u}}du$$

$$\leqslant (k+1)!\,4^{k+3}M\int_{y_0}^{\infty}x^2(\log x)^{k}e^{-x}dx, \qquad (6.188)$$

这里 $y_0=(4+k)\log M$。由 $y_0>2(2+k)$，用分部积分，可以得出

$$\int_{y_0}^{\infty}x^2(\log x)^{k}e^{-x}dx\leqslant y_0^2(\log y_0)^{k}e^{-y_0}$$

$$+\frac{2+k}{y_0}\int_{y_0}^{\infty}x^2(\log x)^{k}e^{-x}dx\leqslant 2y_0^2(\log y_0)^{k}e^{-y_0},$$

由此以及

$$g\geqslant k\geqslant 3,\ M>\frac{1}{4\pi^2}\exp(500g^3),$$

再用(6.138)即得

$$|\Sigma_2|\leqslant 1.$$

引理证毕。

命

$$G\left(s+\frac{1}{2}\right)=\sum_{n=1}^{\infty}g_n n^{-s},\ G\left(s+\frac{1}{2},\ x\right)=\sum_{1<n<x}g_n n^{-s}. \qquad (6.189)$$

以 $P(\xi)$ 表示所有满足 $\chi(p)\neq -1$，且 $p^v\leqslant\xi$ 的素数幂 p^v 的乘积。由(6.174)，有

$$\Psi\left(s+\frac{1}{2}\right)\lll\zeta(2s)^2,\ G\left(s+\frac{1}{2}\right)\lll\left(\frac{\zeta_K(s)}{\zeta(2s)}\right)^2. \qquad (6.190)$$

由(6.190)可知，对 $0<A_1<A$，有

$$G\left(s+\frac{1}{2},\ A\right)\Psi\left(s+\frac{1}{2}\right)=G\left(s+\frac{1}{2},\ A_1\right)\Psi\left(s+\frac{1}{2}\right)$$

$$+\sum_{n=1}^{\infty}c_n n^{-s}, \qquad (6.191)$$

这里，对 $n\leqslant A$，$c_n=0$，除非

$$n = mk_1^2,\ m \mid P(A),\ A_1 \leqslant m \leqslant A, \tag{6.192}$$

而在后一种情况下，有

$$|c_n| \leqslant \sum_{n=mk_1^2} \tau(k_1) \sum_{1<u|m} \nu_n \nu_{\frac{m}{u}},\ \text{如 } n \text{ 满足(6.192)}. \tag{6.193}$$

我们来证明下面的引理。

引理 5.9 设 $d > \exp(500g^3)$。如有 $L(1, \chi) < d^{-\frac{1}{2}}(\log d)^{k-1}$，则

$$\Sigma_1 = \frac{d^k}{ds^k}\left(M^s \Gamma\left(s+\frac{1}{2}\right)^2 G\left(s+\frac{1}{2},\ U\right)\Psi\left(s+\frac{1}{2}\right)\right)\Bigg|_{s=\frac{1}{2}}$$
$$+ O(g^{4g} N L(1, \chi) M (\log\log M)^{k+4}),$$

这里 $U = (\log d)^{8g}$，Σ 如(6.185)所定义，O 所含的正常数是与 g、k、N、d、M 均无关的且可以有效地计算的绝对正常数。

证明 用上面引理的证明方法，不难证明

$$\Sigma_1 = T\left(G\left(s+\frac{1}{2},\ A\right)\right) + o(1), \tag{6.194}$$

这里 $o(1)$ 这一项的绝对值小于等于 1，而对任一函数 $H(s)$，定义

$$T(H(s)) \stackrel{\text{def}}{=} \frac{d^k}{ds^k}\left(\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} M^{s+z}\Gamma\left(s+z+\frac{1}{2}\right)^2\right.$$
$$\left. H(s+z)\Psi\left(s+z+\frac{1}{2}\right)\frac{dz}{z}\right)\Bigg|_{s=\frac{1}{2}}, \tag{6.195}$$

这里还假定 $H(s)$ 是在 $\mathrm{Re}\, s = \sigma \geqslant 2$ 中解析的函数，并满足

$$|F(s)| < c_3(|s|+2)^{c_4},$$

其中 c_3、c_4 是两个固定的正常数。

由(6.191)即知，(6.194)可进一步改为

$$\Sigma_1 = T(G(s,\ A_1)) + \Sigma_3 + O(1), \tag{6.196}$$

$$\Sigma_3 = \sum_{v=0}^{k}\binom{k}{v}\sum_{n<A} c_n \sqrt{\frac{M}{n}}\left(\log\frac{M}{n}\right)^{k-v} I_v\left(\frac{n}{M}\right), \tag{6.197}$$

注意，这里已把所有 $n > A$ 的各项的贡献计入 O-常数项，而后者的绝对值小于等于 1。

现取

$$A_1 = M(\log M)^{-20g},\ A_0 = M((k+6)\log\log M)^2. \tag{6.198}$$

由(6.192)知, $n<A_1$ 时, $c_n=0$。故由(6.197), 有

$$|\Sigma_3| \leqslant \sum_{v=0}^{k} \binom{k}{v} \Big(\sum_{A_1<n<A_0} + \sum_{A_0<n<A} \Big) = S_1 + S_2. \qquad (6.199)$$

用估计(6.184)的第二式可得

$$S_2 \leqslant 2^{k+2}(k+1)!\,\sqrt{M}\left(\log\frac{A}{M}\right)^k (\log M)^{-(k+6)} \sum_{A_0<n<A} |c_n| n^{-\frac{1}{2}}, \qquad (6.200)$$

对此用(6.193), $\tau(k_1) \leqslant \sqrt{3k_1}$ 和引理 5.5 可知, 对任意的 $10<y<\frac{\sqrt{d}}{4}<A_0$, 有

$$\sum_{A_0<n<A} |c_n| n^{-\frac{1}{2}} \leqslant \sum_{k_1^{\frac{1}{2}}<\frac{A}{A_0}} \tau(k_1) k_1^{-1} \sum_{A_0<m<Ak^{-\frac{1}{2}}} m^{-\frac{1}{2}} \sum_{1<u|m} \nu_u \nu_{\frac{m}{u}}$$
$$\ll \left(L(1,\chi)^2 A y^{-\frac{1}{2}} + L(1,\chi) A^{\frac{1}{2}}\right)(\log y)^3,$$

取

$$y = L(1,\chi)^2 A \leqslant (\log d)^{2(k-1)} d^{-1} M((8+2k)\log M)^2$$
$$\leqslant \frac{N}{4\pi^2}(8+2g)^2 (\log M)^{2g},$$

即得

$$\sum_{A_0<n<A} |c_n| n^{-\frac{1}{2}} \ll g^4 (\log(gN))^3 L(1,\chi)\sqrt{M}(\log M)$$
$$(\log\log M)^3,$$

这里"≪"所含正常数是可以有效地计算的绝对正常数, 以此代入(6.200), 即得

$$S_2 \ll g^{4g} (\log N)^3 L(1,\chi) M, \qquad (6.201)$$

这里"≪"所含正常数是可以有效地计算的绝对正常数。

对 S_1, 用估计(6.184)的第一式可得

$$S_1 \leqslant 2^{k+2} k! \left(\log\frac{M}{A_1}\right)^k \sqrt{M} \sum_{A_1<n<A_0} |c_n| n^{-\frac{1}{2}}. \qquad (6.202)$$

令 $10<y<\min\left(A_1, \frac{\sqrt{d}}{4}\right)$, 则由(6.193)及引理 5.5, 有

$$\sum_{A_1<n<A_0} |c_n| n^{-\frac{1}{2}} \leqslant \sum_{k_1^{\frac{1}{2}}<\frac{A_0}{A_1}} \tau(k_1) k_1^{-1} \sum_{A_1<m<A_0 k^{-\frac{1}{2}}} m^{-\frac{1}{2}} \sum_{1<u|m} \nu_u \nu_{\frac{m}{u}}$$

$$\ll (L(1,\ \chi)^2 A_0 y^{-\frac{1}{2}} + L(1,\ \chi) A_0^{\frac{1}{2}}) (\log y)^3,$$

现取

$$y = L(1,\ \chi)^2 A_0 \leqslant \frac{N}{4\pi^2}(g+6)^2(\log M)^{2g},$$

即有

$$\sum_{A_1 < n \leqslant A_0} |c_n| n^{-\frac{1}{2}} \ll g^4(\log(gN))^3 L(1, \chi)\sqrt{M}(\log\log M)^4$$

代入(6 202)，即得

$$S_1 \ll g^{4g}(\log N)^3 L(1,\ \chi) M(\log\log M)^{k+4},$$

因此把 S_1 的这一估计与(6.201)代入(6.199)，再用(6 196)，即有

$$\Sigma_1 = T\left(G\left(s+\frac{1}{2},\ A_1\right)\right)$$
$$+ O(g^{4g}(\log N)^3 L(1,\ \chi) M(\log\log M)^{k+4}), \qquad (6.203)$$

O-所含正常数是可以有效地计算的绝对正常数，它与g、k、N、d、M均无关。

记

$$G\left(s+\frac{1}{2},\ A_1\right) = G\left(s+\frac{1}{2},\ U\right) + g(s),\ U = (\log d)^{8g}. \qquad (6.204)$$

$g(s)$ 可展开为一个 Dirichlet 级数，其第 n 项系数的绝对值不超过

$$\sum_{1 \leqslant u | n} \nu_u \nu_{\frac{n}{u}}.$$

因此，由引理 5.6 可知，在 $\mathrm{Re}s = \sigma = \frac{1}{2} + \delta(\delta > 0)$ 上，有

$$|g(s)| \leqslant \sum_{U < n \leqslant A_1} n^{-\frac{1}{2}} \sum_{1 \leqslant u | n} \nu_u \nu_{\frac{n}{u}}$$
$$\ll (L(1,\ \chi)^2 A_1 U^{-\frac{1}{2}} + L(1,\ \chi) A_1^{\frac{2}{5}} d^{\frac{1}{10}}) (\log U)^3$$
$$\ll g^3 N(\log d)^{-2g-2}(\log N)^{-8g},$$

因此用

$$\left|\Psi\left(s+\frac{1}{2}\right)\right| \leqslant \zeta(\sigma)^2 \leqslant \left(\frac{2}{\sigma-1}\right)^2, \ \mathrm{Re}s=\sigma>1,$$

以及 Cauchy 定理(以下的 C_0 是一个中心在 $s=1$ 处半径为 $\delta\left(0<\delta<\frac{1}{4}\right)$的圆周)可得

$$\begin{aligned} T(g(s)) = &\frac{k!}{2\pi \mathrm{i}}\int_{C_0}\left(s-\frac{1}{2}\right)^{-k-1}\left(\frac{1}{2\pi \mathrm{i}}\int_{2\delta-\mathrm{i}\infty}^{2\delta+\mathrm{i}\infty}\right. \\ &\left.\cdot M^{z+s}\Gamma\left(z+s+\frac{1}{2}\right)^2 g(s+z)\Psi\left(s+z+\frac{1}{2}\right)\frac{dz}{z}\right)ds \\ &\ll k!\, g^3 N\delta^{-k-3} M^{\frac{1}{2}+3\delta}(\log d)^{-\varphi/2}, \end{aligned}$$

注意上面已把内积分的路径移至 $\mathrm{Re}z=2\delta$, 所以

$$\frac{1}{2}+\delta \leqslant \mathrm{Re}(s+\delta) \leqslant \frac{1}{2}+3\delta, \ 如\ s\in C_0.$$

取 $\delta=((\log d)\log N)^{-1}$, 即可有

$$T(g(s)) \ll g^{2\varphi} N M^{\frac{1}{2}}(\log d)^{-\varphi},$$

由此及(6.204)与(6.203)即知,我们已证明了

$$\Sigma_1 = T\left(G\left(s+\frac{1}{2}, U\right)\right)+O(g^{4\varphi}NL(1,\chi)M(\log\log M)^{k+4}), \tag{6.205}$$

这里 O-所含的正常数是可以有效地计算的绝对正常数, 它与 g、k、N、d、M 均无关。

下面来计算 $T\left(G\left(s+\frac{1}{2}, U\right)\right)$. 引理 5.9 由下列断言得出。

断言

$$T\left(G\left(s+\frac{1}{2}, U\right)\right) = \frac{d^k}{ds^k}\left(M^s\Gamma\left(s+\frac{1}{2}\right)^2 G\left(s+\frac{1}{2}, U\right)\Psi\left(s+\frac{1}{2}\right)\right)\Bigg|_{s=\frac{1}{2}} + \theta\sqrt{M},$$

这里 $|\theta|\leqslant 1$.

断言的证明 令 C_δ 为中心在 $s=\frac{1}{2}$ 处,半径为 $\frac{1}{2}\delta>0$ 的圆周,其中 δ 充分小,待定。由 Cauchy 定理知

$$T\left(G\left(s+\frac{1}{2},U\right)\right)=\frac{k!}{2\pi i}\int_{C_\delta}\left(s-\frac{1}{2}\right)^{-k-1}$$

$$\cdot\left(\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}M^{s+z}\Gamma\left(s+z+\frac{1}{2}\right)^2\right.$$

$$\left.\cdot G\left(s+z+\frac{1}{2},U\right)\Psi\left(s+z+\frac{1}{2}\right)\frac{dz}{z}\right)ds, \qquad (6.206)$$

上式的内积分可由在 $z=0$ 处的残数及另一个路径的积分得出，其中残数是

$$R=\frac{d^k}{ds^k}\left(M^s\Gamma\left(s+\frac{1}{2}\right)^2G\left(s+\frac{1}{2},U\right)\Psi\left(s+\frac{1}{2}\right)\right)\Bigg|_{s=\frac{1}{2}},$$

确切地说，有 (6.207)

$$T\left(G\left(s+\frac{1}{2},U\right)\right)=R+\frac{k!}{2\pi i}\int_{C_\delta}\left(s-\frac{1}{2}\right)^{-k-1}\sum_{r=1}^{5}J_r(s)ds, \qquad (6.208)$$

这里

$$J_1=\int_{\frac{1}{8}+iX}^{\frac{1}{8}+i\infty},\quad J_2=\int_{\frac{1}{8}-i\infty}^{\frac{1}{8}-iX},\quad J_3=\int_{\frac{1}{8}-iX}^{-\delta-iX},\quad J_4=\int_{-\delta+iX}^{\frac{1}{8}+iX},$$

$$J_5=\int_{-\delta-iX}^{-\delta+iX},$$

其中 X 是一个充分大的正数，待定。

易知，当 $\mathrm{Re}\,s=\sigma>0$，$t=\mathrm{Im}\,s$ 时，有

$$|\Gamma(s)|\leqslant\sqrt{2\pi}\,e^{\frac{1}{12\sigma}}|s|^{\sigma-\frac{1}{2}}\cdot\begin{cases}e^{-\sigma}, & \text{如}\left|\dfrac{\sigma}{t}\right|\geqslant\dfrac{\pi}{2},\\ e^{-\frac{\pi}{2}|t|}, & \text{如}\left|\dfrac{\sigma}{t}\right|\leqslant\dfrac{\pi}{2}.\end{cases} \qquad (6.209)$$

又当 $\mathrm{Re}(s+z)>0$ 时，有

$$\left|G\left(s+z+\frac{1}{2},U\right)\right|\leqslant\sum_{1\leqslant n\leqslant v}\sum_{1\leqslant u|n}\nu_u\nu_{\frac{n}{u}}\leqslant\sum_{1\leqslant n\leqslant v}n^2\leqslant(\log d)^{24\theta}. \qquad (6.210)$$

由 $\Psi\left(s+\frac{1}{2}\right)\ll\zeta(2s)^2$ 可得

$$\Psi\left(s+\frac{1}{2}\right) \ll \begin{cases} |t|^{c_5}, & \text{如}\ \frac{c_6}{2\log|t|}<\sigma<\frac{3}{4},\ |t|>1; \\ \frac{1}{(2\sigma-1)^2}, & \text{如}\ \frac{3}{8}\leqslant\sigma\leqslant\frac{3}{4},\ |t|\leqslant 1, \end{cases} \tag{6.211}$$

这里 c_5、c_6 与"$\ll$"所含正常数均为可以有效地计算的绝对正常数。

由(6.209)—(6.211)可得

$$J_1、J_2 \ll N^5(\log d)^{24g} M^{\frac{5}{8}+\frac{\delta}{2}} e^{-X}. \tag{6.212}$$

取

$$\delta = \frac{c_7}{\log X} < \frac{1}{2},$$

使

$$\mathrm{Re}(2s+2z) > 1 - \frac{c_6}{\log 3X},\ s \in C_\delta.$$

这里 c_7 为一个可以有效计算的正常数，它只与 X 有关。

这样，可有

$$J_3、J_4 \ll N^5(\log d)^{24g} M^{\frac{5}{8}+\frac{\delta}{2}} e^{-X} \tag{6.213}$$

又不难证明

$$J_5 \ll N^5(\log d)^{24g} M^{\frac{1}{2}(1-\delta)} \delta^{-3}. \tag{6.214}$$

由(6.212)—(6.214)可知，可取充分大的正常数 c_8，它是可以有效地计算的绝对常数，而令

$$X = c_8 g N \log M,$$

即可得到

$$\left| T\left(G\left(s+\frac{1}{2}, U\right)\right) - R \right| \leqslant \sqrt{M}.$$

这样就证明了断言，也就证明了我们的引理。

5.5 Goldfeld 定理的证明(三)

本小节中，我们要最后证明定理 5.2.

首先不妨设

$$L(1,\chi)\leqslant d^{-\frac{1}{2}}(\log d)^{k-1}.$$

由 §5.3 的(6.173)、(6.164)和(6.167)，有

$$\Psi\left(s+\frac{1}{2}\right)=\frac{(2\pi^{\frac{3}{2}}N^{-2})^{2s+1}\tilde{\Lambda}(2s+1)}{\Gamma(2s+1)\Gamma\left(s+\frac{1}{2}\right)\zeta(2s)}\prod_{p\mid N}(1-p^{-2s})^{-1},$$

特别有

$$\Psi\left(s+\frac{1}{2}\right)=8\pi^3N^{-2}\tilde{\Lambda}(2)\prod_{p\mid N}(1-p^{-1})^{-1}\left(s-\frac{1}{2}\right)$$
$$+O\left(\left|s-\frac{1}{2}\right|^2\right),\ s\to\frac{1}{2}.$$

已知 $\tilde{\Lambda}(2)\geqslant 6\times10^{-8}N$(即 (6.172))，所以$\Psi\left(s+\frac{1}{2}\right)$在 $s=\frac{1}{2}$ 处有一个一阶零点，且有

$$\Psi'(1)=8\pi^3N^{-2}\tilde{\Lambda}(2)\prod_{p\mid N}(1-p^{-1})^{-1}\geqslant10^{-5}N^{-1}.\quad(6.215)$$

由(6.187)、引理 5.8 与引理 5.9，即知，当 $d>\exp(500g^3)$ 时，有

$$\frac{d^k}{ds^k}\left(M^s\Gamma\left(s+\frac{1}{2}\right)^2G\left(s+\frac{1}{2},U\right)\Psi\left(s+\frac{1}{2}\right)\right)\Big|_{s=\frac{1}{2}}$$
$$\ll g^{4g}NL(1,\chi)M(\log\log M)^{k+4},\quad(6.216)$$

这里“≪”所含正常数为可以有效计算的绝对正常数，与 g、k、N、d、M 均无关，以下如无特殊声明，都约定是这样的。

以H记(6.216)的左边，则由本小节开头对$\Psi\left(s+\frac{1}{2}\right)$的讨论，可知有

$$H=k\sqrt{M}(\log M)^{k-1}G(1,V)\Psi'(1)$$
$$+\sqrt{M}\sum_{v=2}^{k}\binom{k}{v}(\log M)^{k-v}\frac{d^v}{ds^v}$$
$$\cdot\left(\Gamma\left(s+\frac{1}{2}\right)^2G\left(s+\frac{1}{2},V\right)\Psi\left(s+\frac{1}{2}\right)\right)\Big|_{s=\frac{1}{2}}.\quad(6.217)$$

又对 $2\leqslant v\leqslant k$，有

$$\frac{d^v}{ds^v}\left(\Gamma\left(s+\frac{1}{2}\right)^2G\left(s+\frac{1}{2},V\right)\Psi\left(s+\frac{1}{2}\right)\right)\Big|_{s=\frac{1}{2}}$$

$$=\sum_{l=0}^{v}\binom{v}{l}\frac{d^{v-l}}{ds^{v-l}}\left(\Gamma\left(s+\frac{1}{2}\right)^{2}\Psi\left(s+\frac{1}{2}\right)\right)\Big|_{s=\frac{1}{2}}$$

$$\cdot\frac{d^{l}}{ds^{l}}G\left(s+\frac{1}{2},V\right)\Big|_{s=\frac{1}{2}}. \tag{6.218}$$

由 Cauchy 定理有

$$\left|\frac{d^{l}}{ds^{l}}G\left(s+\frac{1}{2},V\right)\Big|_{s=\frac{1}{2}}\right|$$

$$=\left|\frac{l!}{2\pi i}\int_{|s-\frac{1}{2}|=\frac{1}{4}}\left(s-\frac{1}{2}\right)^{-l-1}G\left(s+\frac{1}{2},V\right)ds\right|$$

$$\leqslant 4^{l}l!\max_{|s-\frac{1}{2}|=\frac{1}{4}}\left|G\left(s+\frac{1}{2},V\right)\right|\leqslant 4^{l}l!\prod_{\substack{\chi(p)=-1\\ p<(\log d)^{8g}}}(1-p^{-\frac{1}{4}})^{-4},$$

这里用了(6.190)的第二式，由此可得

$$\frac{d^{l}}{ds^{l}}G\left(s+\frac{1}{2},V\right)<\exp(100g^{\frac{3}{4}}(\log\log d)^{\frac{3}{4}}), \tag{6.219}$$

最后的这个不等式，可以仿照引理 5.7 的证明方法而得到，我们特别指出，那里已证明至多有$[2g\log\log d]$个小于$(\log d)^{8g}$的素数 p 满足 $\chi(p)=-1$。

同样也有

$$\left|\frac{d^{l}}{ds^{l}}\left(\Gamma\left(s+\frac{1}{2}\right)^{2}\Psi\left(s+\frac{1}{2}\right)\right)\Big|_{s=\frac{1}{2}}\right|$$

$$=\left|\frac{l!}{2\pi i}\int_{|s-\frac{1}{2}|=\frac{1}{8}}\left(s-\frac{1}{2}\right)^{-l-1}\Gamma\left(s+\frac{1}{2}\right)^{2}\Psi\left(s+\frac{1}{2}\right)ds\right|$$

$$\leqslant 8^{l}l!\max_{|s-\frac{1}{2}|=\frac{1}{8}}\left|\Gamma\left(s+\frac{1}{2}\right)^{2}\Psi\left(s+\frac{1}{2}\right)\right|\ll 8^{l}l!, \tag{6.220}$$

这里用了(6.211)以及Γ函数的性质。

因此由(6.217)～(6.220)可得

$$H=k\sqrt{M}(\log M)^{k-1}G(1,V)\Psi'(1)$$

$$+O(g^{8g}\sqrt{M}(\log M)^{k-2}\exp(100g^{\frac{3}{4}}(\log\log d)^{\frac{3}{4}}), \tag{6.221}$$

这里 O-所含正常数是可以有效计算的绝对正常数，它与 k、g、d、N、M 均无关。

我们需要下面的引理。

引理 5.10 $G(1, U) \gg \prod_{\substack{\chi(p) \neq -1 \\ p < (\log d)^{8g}}} (1+p^{-\frac{1}{2}})^{-4}$,

这里"$\gg$"所含正常数是可以有效地计算的绝对正常数，它与 k、g、N、d、M 均无关。

证明 命 $P\left(s+\frac{1}{2}, U\right)$为 $G\left(s+\frac{1}{2}\right)$ 的由小于等于U的素数 p所确定的部分 Euler 乘积，那么有

$$G\left(s+\frac{1}{2}, U\right) = P\left(s+\frac{1}{2}, U\right) - R\left(s+\frac{1}{2}, U\right). \quad (6.222)$$

由 $G(s)$的定义(6.173)有

$$P(1, U) \geqslant \prod_{\substack{\chi(p) \neq -1 \\ p < U}} (1+p^{-\frac{1}{2}})^{-4}, \quad (6.223)$$

令

$$\mathfrak{M}_U = \{1 \leqslant n \in \mathbb{Z} \mid \text{素数 } p \mid n \Rightarrow p \leqslant U\}, \quad (6.224)$$

则有

$$R\left(s+\frac{1}{2}, U\right) = \sum_{\substack{n > U \\ n \in \mathfrak{M}_u}} g_n n^{-s},$$

这里用了定义(6.189)。

这样就有

$$|R(1, U)| \leqslant \sum_{U < n < \frac{\sqrt{d}}{4}} |g_n| n^{-\frac{1}{2}} + \sum_{\substack{n > \frac{\sqrt{d}}{4} \\ n \in \mathfrak{M}_u}} |g_n| n^{-\frac{1}{2}} = R_1 + R_2. \quad (6.225)$$

由(6.190)的第二式可得

$$R_1 \leqslant U^{-\frac{1}{2}} \Big(\sum_{1 < n < \frac{\sqrt{d}}{4}} \nu_n \Big)^2 \ll U^{-\frac{1}{2}} (\log d)^{2g} = (\log d)^{-2g}, \quad (6.226)$$

这里用到了引理 5.3。

为估计 R_2，我们指出

$$R_2 \leqslant \lim_{x \to \infty} \sum_{\substack{1 \leqslant n < x \\ n \in \mathfrak{M} U}} |g_n| n^{-\frac{1}{2}} \left(1 - \frac{n}{x}\right) - \sum_{\substack{1 < n < \frac{\sqrt{d}}{4} \\ n \in \mathfrak{M} U}} |g_n| n^{-\frac{1}{2}} \left(1 - \frac{4n}{\sqrt{d}}\right),$$

由此及下列容易证明的事实

$$R\left(s+\frac{1}{2}, U\right) \ll P_1\left(s+\frac{1}{2}, U\right) \stackrel{\text{def}}{=} \prod_{\substack{\chi(p)=-1 \\ p<U}} (1-p^{-s})^{-4},$$

可得

$$R_2 \leqslant \lim_{x\to\infty} \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} P_1(1+z, U)\frac{x^z-\left(\frac{\sqrt{d}}{4}\right)^z}{z(z+1)}dz$$

$$\ll \lim_{x\to\infty} P_1\left(\frac{1}{2}, U\right)(x^{-\frac{1}{2}}+d^{-\frac{1}{4}}) \ll d^{-\frac{1}{4}}(\log d)^{4g}, \quad (6.227)$$

这里用到

$$2^{|\mathscr{F}|} \leqslant \frac{1}{2\log 2.5}(\log d)^{k-1},$$

这可在引理 5.7 的证明过程中得到。

于是，由(6.222)～(6.227)得到

$$|G(1, U)| \geqslant \prod_{\substack{\chi(p)\neq -1 \\ p<U}} (1+p^{-\frac{1}{2}})^{-4} + O((\log d)^{-2g}),$$

但由引理 5.7 已知上式的右边的乘积大于$\exp(-20\sqrt{g\log\log d})$，所以这就证明了引理 5.10。

由(6.215)和(6.221)，以及引理 5.10，可得

$$H \gg k\sqrt{M}(\log M)^{k-1}N^{-1}\prod_{\substack{\chi(p)\neq -1 \\ p<(\log d)^{8g}}} (1+p^{-\frac{1}{2}})^{-4}$$

$$-c_9 g^{8g}\sqrt{M}(\log M)^{k-2}\exp(100(g\log\log d)^{\frac{3}{4}}), \quad (6.228)$$

这里"$\gg$"所含正常数与 c_9 均为可以有效地计算的绝对正常数，它们与 k、g、N、d、M 均无关。

因此由(6.228)可知，只要取 c_1 充分大(仍是一个可以有效地计算的绝对正常数，与g、N、d、k、M 均无关)，当$d>\exp\exp(c_1 N g^3)$时，即有

$$H \gg g\sqrt{M}(\log M)^{k-1}N^{-1}\prod_{\substack{\chi(p)\neq -1 \\ p<(\log d)^{8g}}} (1+p^{-\frac{1}{2}})^{-4},$$

最后，结合(6.216)，得到

$$L(1, \chi) \gg \frac{c_2}{g^{4g}N^3}\cdot\frac{(\log d)^{k-1}}{(\log\log d)^{k+4}}\prod_{\substack{\chi(p)\neq -1 \\ p<(\log d)^{8g}}} (1+p^{-\frac{1}{2}})^{-4},$$

此即定理5.2。

终于完成了Goldfeld定理的证明。

本 章 评 注

1. Gauss猜想存在无穷多个类数为1的实二次域。这是一个非常困难的问题。至今尚未看到解决这一问题的任何线索。我们在第一节中对此作了一些讨论，有关结果，除个别以外，是本书首次阐述的。

2. 对于实二次域类数为1的判别准则，有相当一部分数学家研究过这一问题。例如，有Ankeny, Hasse, Chowla[2]等人。我们用连分数给出的这些准则，取自我们1979年来发表的一系列论文[46~53]。这些工作的某些方面后来又为A.Mollin、C.Williams, H.Yokoi.G.Lachaud(例如，可见参考文献[80]的介绍)所重新发现。

3. 用连分数来表出虚二次域的类数，与实二次域的研究有很大关系。这方面的第一个工作是F. Hirzebruch于1973年首先给出的(参阅参考文献[116])。后来我们在1983年以后的一系列工作[52~62]中，把这个Hirzebruch-Zagier类数公式做了许多扩张。这就是第三节的内容，最近我们[70~71]又有了一些新的进展，限于篇幅，没有写入本书。

4. 第四节讨论的S.Chowla的一个猜想，A.Mollin与C.Williams[76~79]也作了很好的探讨，两者之间各有所长。我们这里的讨论似乎更为充分得多，但目前尚未看到这一猜想在近期被解决的可能性。我们的方法还可用到类似的实二次域的研究中去。

5. 第五节的Goldfeld定理与上一章的关系是很紧密的，但由于实二次域与虚二次域有本质的不同，所以证明方法是有所不同的。我们把Goldfeld的原始证明中的若干不够明显的地方作了澄清，对于有兴趣的读者会是有用的。然而要找到满足BSD弱

猜想的秩为 4 的椭圆曲线，目前尚无可能。可做的事情是把定理中的两个有效常数 c_1、c_2 明确地定下来，当然是应该尽可能地好。

第 7 章

Hirzebruch 和与 Hecke 算子

对每一个实二次无理数α，用它的简单连分数展开式，我们在第三章中定义了一个所谓的 Hirzebruch 和。我们发现这个和在 Hecke 算子下的变化，有点像固有函数，而相应的固有值与α所属二次域的正则子有密切关系。本章叙述这一现象，在第一节中首先介绍对一个素数p，实二次域$Q(\sqrt{p})$的基本单位

$$\varepsilon_p = \frac{t+u\sqrt{p}}{2}$$

结构的两个有关猜想，即是 Ankeny-Artin-Chowla 和 Mordell猜想：$p \nmid u$。第二节证明 Hirzebruch 和的一个恒等式。第三、四节分别给出在两个特殊情况下，Hirzebruch 和在 Hecke 算子作用下的固有值与上述两个猜想的关系。

§1 实二次域基本单位的两个著名猜想

实二次域的基本单位是个很难的研究对象，除了对给定的域，可以用连分数来算出它之外，几乎没有什么话可说。N.C.Ankeny，E.Artin 和 S.Chowla 以及 L.J.Mordell 分别在 1952 年参考文献[1]和 1960 年参考文献[83]中提出两个著名猜想，它们很类似，现在我们叙述如下：

猜想 1 (Ankeny-Artin-Chowal) 设素数$p\equiv 1 \pmod 4$，令 Pell 方程

$$x^2 - py^2 = -4,\ x,\ y \in \mathbb{Z}$$

的基本解为

$$\varepsilon_p=\frac{t+u\sqrt{p}}{2},$$

则 $p\nmid u$。

猜想 2(L. J. Mordell) 设素数 $p\equiv 3 \pmod 4$，令 Pell 方程

$$x^2-py^2=1,\ x,\ y\in Z$$

的基本解为

$$\varepsilon_p=t+u\sqrt{p},$$

则 $p\nmid u$。

附注 显然 ε_p 均是相应的实二次域 $Q(\sqrt{p})$ 的基本单位。

虽然对 $p\leqslant 10^5$，当 $p\equiv 1 \pmod 8$；$p\leqslant 2000$，当 $p\equiv 5 \pmod 8$；$p\leqslant 18000$，当 $p\equiv 3 \pmod 4$ 时，已分别验证了上述两个猜想的正确性。但对一般的素数 p，似乎还看不到处理它们的线索。我们将在本章中把这两个猜想与 Hirzebruch 和在 Hecke 算子作用下的固有值联系起来，这也许会给这两个猜想的研究带来一线希望。

我们提一下以下的两个结果：

定理 1.1 在猜想 1, 2 的记号下，我们有下列的结论。

(1) 当素数 $p\equiv 1 \pmod 4$ 时，

$$h(p)u\equiv tB_{\frac{p-1}{2}} \pmod p;$$

(2) 当素数 $p\equiv 3 \pmod 4$ 时，

$$4h(p)u\equiv(-1)^{\frac{p-3}{4}}tE_{\frac{p-3}{4}} \pmod p.$$

以上 $h(p)$ 是 $Q(\sqrt{p})$ 的类数，B_n 与 E_n 分别是 Bernoulli 数与 Euler 数。

定理的证明可参阅参考文献[50]。

§2 Hirzebruch和的一个恒等式

本节给出 Hirzebruch 和的一个恒等式及其证明。由于证明的需要，所以首先在第一小节中叙述并证明 Dedekind 和的一个

Petersson-Knopp 恒等式。然后在第二小节中利用后一恒等式给出第一个恒等式的证明。

2.1 Petersson-Knopp 恒等式

定理 2.1 对 $h, k, n\in \mathbb{Z}$, $k, n\geqslant 1$, 我们有恒等式

$$\sum_{\substack{ad=n\\ d>0}}\sum_{b(\bmod d)} s(ah+bk, dk)=\sigma(n)s(h, k),$$

这里 $a, b, d\in \mathbb{Z}$; $\sigma(n)$ 是 n 的正因子的和; $s(h, k)$是 Dedekind 和,并对 $g.c.d.(h, k)>1$ 也有定义:

$$s(hm, km)=s(h, k),\ 如\ m\in \mathbb{N}. \tag{7.1}$$

证明 已知对 Dedekind η 函数有

$$\log\eta(\tau)=\frac{\pi i\tau}{12}-\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{2\pi in\tau},\ \operatorname{Im}\tau>0. \tag{7.2}$$

因此,对任一个素数 p, 有

$$\begin{aligned}\log\eta(p\tau)+\sum_{b=0}^{p-1}\log\eta\left(\frac{\tau+b}{p}\right)&=\frac{\pi ip\tau}{12}+\sum_{b=0}^{p-1}\frac{\pi i}{12p}(\tau+b)\\ &-\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{2\pi inp\tau}-\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{2\pi in\tau/p}\sum_{b=0}^{p-1}e^{2\pi inb/p}\\ &=\frac{(p+1)\pi i\tau}{12}+\frac{(p-1)\pi i}{24}-\sum_{n=1}^{\infty}\frac{\sigma(n)}{n}e^{2\pi inp\tau}\\ &-\sum_{n=1}^{\infty}\frac{\sigma(pn)}{n}e^{2\pi in\tau}.\end{aligned} \tag{7.3}$$

命 $n=p^m n'$, $p\nmid n'$, 则由(7.3)可得

$$\begin{aligned}\log\eta(p\tau)+\sum_{b=0}^{p-1}\log\eta\left(\frac{\tau+b}{p}\right)&=\frac{(p+1)\pi i\tau}{12}+\frac{(p-1)\pi i}{24}\\ &-\sum_{\substack{n=1\\ p\nmid n}}^{\infty}\sum_{l=0}^{\infty}\frac{\sigma(n)\sigma(p^l)}{np^l}e^{2\pi inp^{l+1}\tau}\\ &-\sum_{\substack{n=1\\ p\nmid n}}^{\infty}\sum_{l=0}^{\infty}\frac{\sigma(n)\sigma(p^{l+1})}{np^l}e^{2\pi inp^l\tau},\end{aligned}$$

由此及

$$\sigma(p)=p+1,\ \frac{\sigma(p^{l+1})}{p^l}+\frac{\sigma(p^{l-1})}{p^{l-1}}=(p+1)\frac{\sigma(p^l)}{p^l}\ (l\geqslant 1),$$

即得

$$\log\eta(p\tau)+\sum_{b=0}^{p-1}\log\eta\left(\frac{\tau+b}{p}\right)=\sigma(p)\log\eta(\tau)+\frac{(p-1)\pi i}{24}. \tag{7.4}$$

由(7.1)可知，我们可设 $h, k\in\mathbb{Z}$, $k\geqslant 1$, $g.c.d.(h, k)=1$. 可取 $\alpha, \beta\in\mathbb{Z}$, 使 $\alpha h-\beta k=1$.

容易看出

$$\begin{pmatrix}p&0\\0&1\end{pmatrix}\begin{pmatrix}\alpha&\beta\\k&h\end{pmatrix}=\begin{cases}\begin{pmatrix}\alpha&p\beta\\\frac{k}{p}&h\end{pmatrix}\begin{pmatrix}p&0\\0&1\end{pmatrix}, & \text{如 } p\mid k;\\ \begin{pmatrix}p\alpha&\beta-\alpha b\\k&\frac{h-bk}{p}\end{pmatrix}\begin{pmatrix}1&b\\0&p\end{pmatrix}, & \text{如 } p\nmid k, \text{ 而 } b \text{ 满足 } 0\leqslant b\leqslant p-1, \text{ 以及 } p\mid h-bk,\end{cases}$$

$$\begin{pmatrix}1&b\\0&p\end{pmatrix}\begin{pmatrix}\alpha&\beta\\k&h\end{pmatrix}=\begin{cases}\begin{pmatrix}\frac{\alpha+bk}{p}&\beta+bh\\k&ph\end{pmatrix}\begin{pmatrix}p&0\\0&1\end{pmatrix}, & \text{如 } p\mid\alpha+bk;\\ \begin{pmatrix}\alpha+bk&\frac{\beta+bh-b_1(\alpha+bk)}{p}\\pk&h-b_1k\end{pmatrix}\begin{pmatrix}1&b_1\\0&p\end{pmatrix}, & \end{cases}$$

如 $p\nmid\alpha+bk$, b_1 满足 $0\leqslant b_1\leqslant p-1$, $p\mid\beta+bh-b_1(\alpha+bk)$, 因此可知，对 $ad=p$, $a, b, d\in\mathbb{Z}$, $d>0$, $0\leqslant b\leqslant d-1$, 存在 α', β', h', k', a', d', $b'\in\mathbb{Z}$, 使有

$$\begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}\alpha&\beta\\k&h\end{pmatrix}=\begin{pmatrix}\alpha'&\beta'\\k'&h'\end{pmatrix}\begin{pmatrix}a'&b'\\0&d'\end{pmatrix}, \tag{7.5}$$

$a'd'=p$, $a', b', d'\in\mathbb{Z}$, $0\leqslant b'\leqslant d'-1$, $k'>0$, $d'>0$.

命

$$M=\begin{pmatrix}a&b\\0&d\end{pmatrix},\ V=\begin{pmatrix}\alpha&\beta\\k&h\end{pmatrix},\ M'=\begin{pmatrix}a'&b'\\0&d'\end{pmatrix},\ V'=\begin{pmatrix}\alpha'&\beta'\\k'&h'\end{pmatrix},$$

则有 $V, V'\in SL_2(\mathbb{Z})$ 与 $MV=V'M'$, 以及

$$\left.\begin{aligned}&\alpha'=\frac{d'}{p}(a\alpha+bk),\ k'=\frac{dd'k}{p},\ h'=\frac{a'dh-b'dk}{p},\\&(k'M'\langle\tau\rangle+h')d'=(k\tau+h)d,\end{aligned}\right\} \tag{7.6}$$

由此及 $\log\eta(\tau)$ 的变换公式(见第三章定理 1.1) 可有

$$\log\eta(MV\langle\tau\rangle)=\log\eta(V'M'\langle\tau\rangle)=\log\eta(M'\langle\tau\rangle)$$

$$+\frac{1}{2}\log(-\mathrm{i}(k'M'\langle\tau\rangle+h'))+\frac{\pi\mathrm{i}}{12k'}(h'+\alpha')-\mathrm{i}\pi s(h',k')$$

$$=\log\eta(M'\langle\tau\rangle)+\log\left(\frac{-\mathrm{i}(k\tau+h)d}{d'}\right)-\mathrm{i}\pi s(h',k')$$

$$+\frac{\pi\mathrm{i}p}{12dd'k}\left(\frac{a'dh-b'dk}{p}+\frac{ad'\alpha+bd'k}{p}\right)$$

$$=\log\eta(M'\langle\tau\rangle)+\frac{1}{2}\log(-i(k\tau+h))+\frac{1}{2}(\log d-\log d')$$

$$+\frac{\pi\mathrm{i}}{12}\left(\frac{a'h}{d'k}+\frac{a\alpha}{dk}+\frac{b}{d}-\frac{b'}{d'}\right)-\mathrm{i}\pi s(h',k'),$$

在上式两边对 $ad=p$, $d>0$, $0\leqslant b\leqslant d-1$ 求和, 并用(7.6)即有

$$\sum s(h',k')=\frac{\sigma(p)}{\pi\mathrm{i}}\left[\log\eta(\tau)+\frac{1}{2}\log(-i(k\tau+h))+\frac{\pi\mathrm{i}(\alpha+h)}{12k}-\log\eta(V\langle\tau\rangle)\right]\tag{7.7}$$

这里还用到了下列事实, 对固定的 V、M, 用对应(7.5)所得的 V'、M' 是唯一的。

对(7.7)的右边再用 $\log\eta(\tau)$ 的变换公式, 而对左边用(7.6)可得

$$\sigma(p)s(h,k)=\sum s(h',k')=\sum s\left(\frac{a'dh-b'dk}{p},\ \frac{dd'k}{p}\right)$$

$$=\sum s(a'dh-b'dk,\ dd'k)=\sum s(a'h-b'k,\ d'k)$$

$$=\sum_{\substack{ad=p\\ d>0}}\sum_{b=0}^{d-1}s(ah+bk,\ dk).\tag{7.8}$$

这里用了(7.1)与 $s(h+k,k)=s(h,k)$。

由(7.8)即知定理 2.1 对 $n=p$(素数)是成立的。

对 h, $k\in\mathbb{Z}$, $k>0$, 令

$$f\left(\frac{h}{k}\right)=s(h,k),\tag{7.9}$$

则由(7.1)知定义(7.9)是合理的, 且有

$$f(x+1)=f(x),\ x\in\mathbb{Q}.\tag{7.10}$$

对任一个正整数 n，定义 Hecke 算子 $T_1(n)$ 如下：

$$(T_1(n)F)(x) = \frac{1}{n}\sum_{\substack{ad=n\\ d>0}}\sum_{b(\bmod d)} F\left(\frac{ax+b}{d}\right), \tag{7.11}$$

这里 $a, d, b\in \mathbb{Z}$；F 是定义在 $\mathbf{Q}$ 上的周期为 1 的函数。

容易证明有：

$$(T_1(p)T_1(p^l)F)(x) = (T_1(p^{l+1})F)(x)$$

$$+\frac{1}{p}(T_1(p^{l-1})F)(x)，如 p 为素数，l 为正整数， \tag{7.12}$$

$$T_1(mn) = T_1(m)T_1(n)，如 m, n 为互素的正整数， \tag{7.13}$$

$$T_1(m)T_1(n) = T_1(n)T_1(m)，如 m, n 为正整数， \tag{7.14}$$

在定义了(7.10)与(7.11)下，定理 2.1 可改写为下面的形式。

定理 2.1′　对任一个正整数 n，我们有

$$(T_1(n)f)(x) = \frac{\sigma(n)}{n}f(x). \tag{7.15}$$

由 $T_1(n)$，n，$\sigma(n)$ 的积性可知，只需对素数幂 p^l 来证明定理 2.1′。$l=0$ 时，(7.15) 显然成立；$l=1$ 时，上述的讨论，即由 (7.8) 知，(7.15) 也已成立。以下用归纳法，即对 $l\geqslant 2$，假设 (7.15) 对 $l-1$，$l-2$ 已成立，即假设已有

$$(T_1(p^{l-2})f)\left(\frac{h}{k}\right) = \frac{\sigma(p^{l-2})}{p^{l-2}}f\left(\frac{h}{k}\right),$$

$$(T_1(p^{l-1})f)\left(\frac{h}{k}\right) = \frac{\sigma(p^{l-1})}{p^{l-1}}f\left(\frac{h}{k}\right),$$

则由 (7.12) 即知有

$$\begin{aligned}(T_1(p^l)f)\left(\frac{h}{k}\right) &= (T_1(p)T_1(p^{l-1})f)\left(\frac{h}{k}\right)\\ &\quad -\frac{1}{p}(T_1(p^{l-2})f)\left(\frac{h}{k}\right)\\ &= \left(\frac{\sigma(p^{l-1})\sigma(p)}{p^l} - \frac{p\sigma(p^{l-2})}{p^l}\right)f\left(\frac{h}{k}\right)\\ &= \frac{\sigma(p^l)}{p^l}f\left(\frac{h}{k}\right),\end{aligned}$$

这就完成了归纳步骤。由归纳法即知定理 2.1′ 已经成立，从而定

理 2.1 获证。

附注 我们也可改写定理 2.1′ 为下面的形式。

定理 2.1″ 对任一个正整数 n，我们有

$$(T(n)f)(x)=\sigma(n)f(x),$$

这里 $T(n)=nT_1(n)$。

2.2 Hirzebruch 和的一个恒等式

本小节中，我们要证明下面的定理 2.2。

定理 2.2 设 $D=B^2+4AC$ 是一个非完全平方的正整数，其中 $A, B, C\in\mathbb{Z}$，$A>0$，且 $g.c.d.(A, B, C)=1$。则对任一个正整数 N 及任一个实二次无理数 $\alpha=\frac{B+\sqrt{D}}{2A}$，有

$$\sum_{\substack{mn=N\\ 1<m,n\in\mathbb{Z}\\ w(\mathrm{mod}\, m)}} J(DN^2; DN^2(g.c.d.(Am^2, BN+2Amn, Aw^2+Bnw-Cn^2))^{-2})\cdot\Psi\left(\frac{n\alpha+w}{m}\right)=\sigma(N)J(DN^2; D)\Psi(\alpha),$$

这里 $\sigma(N)$ 为 N 的正因子的和；对一个实二次无理数 β，$\Psi(\beta)$ 是其 Hirzebruch 和；$J(DN^2; D)$ 定义为

$$J(DN^2; D)=\frac{\log\varepsilon_{DN^2}}{\log\varepsilon_D},$$

这里，对一个非完全平方的正整数 D_1，ε_{D_1} 是 Pell 方程

$$x^2-D_1y^2=4,\ x,\ y\in\mathbb{Z}$$

的基本解。由定义知 $J(DN^2; D)$ 显然是一个正整数。

证明 取模方阵

$$M_\alpha=\begin{pmatrix}\frac{t+BNu}{2} & CNu\\ ANu & \frac{t-BNu}{2}\end{pmatrix}\in SL_2(\mathbb{Z}),$$

$$M_{n,m,w,\alpha}=\begin{pmatrix}\frac{t+BNu}{2}+Amuw & -u(Aw^2+Bwn-Cn^2)\\ Am^2u & \frac{t-BNu}{2}-Amuw\end{pmatrix}\in SL_2(\mathbb{Z}),$$

其中已设 Pell 方程

$$x^2-DN^2y^2=4,\ x,\ y\in\mathbb{Z}$$

的基本解

$$\varepsilon_{DN^2}=\frac{t+uN\sqrt{D}}{2},$$

它等于 $\varepsilon_D^{J(DN^2;D)}$，这里 $\varepsilon_D=\dfrac{t_0+u_0\sqrt{D}}{2}$ 是 Pell 方程

$$x^2-Dy^2=4,\ x,\ y\in\mathbb{Z}$$

的基本解

用第三章的定理 1.2, 由于 M_α 与 $M_{n,m,w,\alpha}$ 均为双曲元, 可得

$$3+J(DN^2;D)\Psi(\alpha)=\frac{t}{ANu}-12s\left(\frac{t-BNu}{2},\ ANu\right)\tag{7.16}$$

与

$$\begin{aligned}&3+J(DN^2;DN^2)g.c.d.(Am^2,\ BN+2Amn,\ Aw^2+Bnw\\&\qquad-Cn^2))^{-2})\Psi\left(\frac{n\alpha+w}{m}\right)\\&=\frac{t}{Aum^2}-12s\left(\frac{t-BNu}{2}-Amuw,\ Aum^2\right).\end{aligned}\tag{7.17}$$

对(7.17)求和, 并用定理 2.1, 即有

$$\begin{aligned}3\sigma(N)+&\sum_{\substack{mn=N\\1\leqslant m,n\in\mathbb{Z}\\w(\mathrm{mod}\,m)}}J(n,\ m,\ w,\ \alpha)\Psi\left(\frac{n\alpha+w}{m}\right)=\sum_{\substack{mn=N\\1\leqslant m,n\in\mathbb{Z}\\w(\mathrm{mod}\,m)}}\frac{t}{Aum^2}\\&-12\sum_{\substack{mn=N\\1\leqslant m,n\in\mathbb{Z}\\w(\mathrm{mod}\,m)}}s\left(\frac{t-BNu}{2}-Amuw,\ Aum^2\right)\\&=\frac{t\sigma(N)}{AuN}-12\sum_{\substack{mn=N\\1\leqslant m,n\in\mathbb{Z}\\w(\mathrm{mod}\,m)}}s\left(n\left(\frac{t-BNu}{2}-Amuw\right),\ nAum^2\right)\\&=\frac{t\sigma(N)}{AuN}-12\sum_{\substack{mn=N\\1\leqslant m,n\in\mathbb{Z}\\w(\mathrm{mod}\,m)}}s\left(n\frac{t-BNu}{2}+ANuw,\ ANum\right)\\&=\frac{t\sigma(N)}{AuN}-12\sigma(N)s\left(\frac{t-BNu}{2},\ ANu\right)\\&=\sigma(N)(3+J(DN^2;D)\Psi(\alpha),\end{aligned}\tag{7.18}$$

这里已简记

$$J(n,\ m,\ w,\ \alpha)=J(DN^2;\ DN^2(g.c.d.(Am^2,\ BN+2Amn,\ Aw^2+Bwn-Cn^2))^{-2}),\qquad(7.19)$$

并在最后一步中用了(7.16)。

由(7.18)即知定理 2.2 已经完全证明。

附注 (7.19)的简略记号以后将经常使用。

§3 AAC 猜想与 Hirzebruch 和

本节中我们讨论 AAC 猜想与 Hirzebruch 和的关系。

首先证明下面的定理。

定理 3.1 设素数 $p\equiv1\pmod 4$，$\alpha=\dfrac{b+\sqrt{4p}}{a}$，其中有理数 a，b 满足

$$a>0,\ g.c.d.(a,\ 2p)=1,\ a|4p-b^2.$$

那么我们有

$$(T(p)\Psi)(\alpha)=(pg_p+1)\Psi(\alpha),\ T(p)=pT_1(p).$$

这里 $T_1(p)$ 为(7.11)定义的 Hecke 算子；

$$g_p=\begin{cases}1, & 如\ p|u;\\ p, & 如\ p\nmid u,\end{cases}$$

其中已设实二次域 $Q(\sqrt{p})$ 的基本单位为

$$\varepsilon=\frac{t+u\sqrt{p}}{2}.$$

证明 在定理 2.2 中取

$$A=a,\ B=2b,\ C=\frac{4p-b^2}{a},\ D=B^2+4AC=16p,\ N=p.$$

易见 $g.c.d.(A,\ B,\ C)=1$。容易算出

$$J(DN^2;\ D)=g_p,$$

$$J(n,\ m,w,\ \alpha)=\begin{cases}1, & 如\ n=p,\ m=1,\ w=0,\ 或\ n=1,\\ & \quad m=p,\ 0\leqslant w\leqslant p-1,\ 而\ p\nmid aw+b;\\ g_p, & 如\ n=1,\ m=p,\ 0\leqslant w\leqslant p-1,\\ & \quad 而\ p|aw+b,\end{cases}$$

这里已采用(7.19)的简略记号。这样，由定理 2.2 可得

$$(T(p)\Psi)(\alpha)=(p+1)g_p\Psi(\alpha)+(1-g_p)\Psi\left(\frac{aw_0+b+\sqrt{4p}}{ap}\right), \tag{7.20}$$

其中有理整数 w_0 满足

$$aw_0+b\equiv 0(\mathrm{mod}\ p).$$

令 $aw_0+b=np$, $n\in\mathbf{Z}$, 则有

$$a(aw_0^2+2bw_0-C)=(aw_0+b)^2-4p=(n^2p-4)p,$$

因此有

$$n^2p-4=ad,\ d\in\mathbf{Z},$$
$$aw_0^2+2bw_0-C=dp.$$

并可有

$$nb-4=a(d-w_0n).$$

由于素数 $p\equiv 1(\mathrm{mod}\ 4)$, 存在 $x, y\in\mathbf{Z}$ 使

$$x^2-py^2=-1.$$

易见 $2|x$, $2\nmid y$。令 $x=2x_0$, $x_0\in\mathbf{Z}$。则有

$$4x_0^2-py^2=-1.$$

命

$\widetilde{A}=y-x_0n$, $\widetilde{B}=w_0y+(d-w_0n)x_0$, $\widetilde{C}=-ax_0$, $\widetilde{D}=py+bx_0$,

则有 $\widetilde{A}\widetilde{D}-\widetilde{B}\widetilde{C}=py^2-4x_0^2=1$, 所以

$$\widetilde{M}=\begin{pmatrix}\widetilde{A} & \widetilde{B}\\ \widetilde{C} & \widetilde{D}\end{pmatrix}\in SL_2(\mathbf{Z}).$$

容易算出

$$\widetilde{M}\langle\alpha\rangle=\frac{aw_0+b+\sqrt{4p}}{ap},$$

这样，由 Hirzebruch 和的定义有

$$\Psi\left(\frac{aw_0+b+\sqrt{4p}}{ap}\right)=\Psi(\alpha), \tag{7.21}$$

由(7.20)与(7.21)即得定理 3.1。

推论 如对一个素数 $p\equiv 1(\mathrm{mod}\ 4)$ AAC 猜想成立，则有

$$\Psi(p\sqrt{4p})=p\Psi(\sqrt{4p}).$$

证明　在推论的假设下，有 $g_p = p$。从而 Pell 方程

$$x^2-4py^2=1,\ x,\ y\in\mathbb{Z}$$

的基本解 $t+u\sqrt{p}$ 满足 $p\nmid u$。由此可知，由

$$(t+u\sqrt{4p})^j=t_j+u_j\sqrt{4p}\ (1\leqslant j\leqslant p-1)$$

定义的有理整数 u_j 满足

$$p\nmid u_j,\ 1\leqslant j\leqslant p-1.$$

由此不难证明下列两个集合的相同。

$$\left\{\frac{t_j}{u_j}(\bmod p),\ 1\leqslant j\leqslant p-1\right\}=\{j(\bmod p),\ 1\leqslant j\leqslant p-1\}.$$

从而，对任给的有理整数 w，如有 $w\not\equiv 0(\bmod\ p)$，则存在一个 j_0，$1\leqslant j_0\leqslant p-1$，使

$$u_{j_0}w+t_{j_0}\equiv 0(\bmod\ p).$$

令

$$\widetilde{A}=\frac{wu_{j_0}+t_{j_0}}{p},\ \widetilde{B}=wt_{j_0}+4pu_{j_0},\ \widetilde{C}=u_{j_0},\ \widetilde{D}=pt_{j_0},$$

则有　$\widetilde{A}\widetilde{D}-\widetilde{B}\widetilde{C}=t_{j_0}^2-4pu_{j_0}^2=1$，从而

$$\widetilde{M}=\begin{pmatrix}\widetilde{A} & \widetilde{B}\\ \widetilde{C} & \widetilde{D}\end{pmatrix}\in SL_2(\mathbb{Z}),$$

容易验证：

$$\widetilde{M}\langle p\sqrt{4p}\rangle=\frac{w+\sqrt{4p}}{p},$$

因此得到

$$\Psi\left(\frac{w+\sqrt{4p}}{p}\right)=\Psi(p\sqrt{4p}),\ 如\ 1\leqslant w\leqslant p-1. \quad (7.22)$$

在定理 3.1 中，取 $a=1$，$b=0$，并用(7.22)，可得

$$(p^2+1)\Psi(\sqrt{4p})=p\Psi(p\sqrt{4p})+\Psi\left(\frac{2}{\sqrt{p}}\right). \quad (7.23)$$

再在定理 2.2 中取 $A=1$，$B=0$，$C=p$，$N=2$，则有 $D=4p$，$\alpha=\sqrt{p}$，由于(仍用简化记号(7.19))

$$J(n,\ m,\ w,\ \alpha)=\begin{cases}1, & 如\ n=2,\ m=1;\\ 1, & 如\ n=1,\ m=2,\ w=0;\\ 4, & 如\ n=1,\ m=2,\ w=1,\end{cases}$$

所以由定理 2.2 有

$$\Psi(2\sqrt{p})+\Psi\left(\frac{\sqrt{p}}{2}\right)+J(16p;p)\Psi\left(\frac{1+\sqrt{p}}{2}\right)$$
$$=3J(16p;4p)\Psi(\sqrt{p}), \tag{7.24}$$

由于 $\sqrt{p}$ 与 $\frac{1+\sqrt{p}}{2}$ 的简单连分数展开式基本周期的长度均是奇数，故由定义有

$$\Psi(\sqrt{p})=\Psi\left(\frac{1+\sqrt{p}}{2}\right)=0. \tag{7.25}$$

这样由 (7.24) 与 (7.25) 即有

$$\Psi\left(\frac{\sqrt{p}}{2}\right)=-\Psi(2\sqrt{p}),$$

结合显然的事实

$$\Psi\left(\frac{2}{\sqrt{p}}\right)=-\Psi\left(\frac{\sqrt{p}}{2}\right),$$

即得

$$\Psi\left(\frac{2}{\sqrt{p}}\right)=\Psi(2\sqrt{p})=\Psi(\sqrt{4p}). \tag{7.26}$$

由 (7.23) 与 (7.26) 即得所需的结论。推论证毕。

下面我们再来证明定理 3.2。

定理 3.2 设素数 $p\equiv1(\bmod 4)$，$\varepsilon_p=\frac{t+u\sqrt{p}}{2}$ 是实二次域 $\boldsymbol{Q}(\sqrt{p})$ 的基本单位。非负整数 ω 由下式定义

$$p^{\omega}\|u.$$

那么我们有：

(1) 对任一个非负整数 k，有

$$(T(p^k)\Psi)(2\sqrt{p})=\lambda_k\Psi(2\sqrt{p}),\ T(n)=nT_1(n),$$

其中 $T_1(n)$ 由 (7.11) 定义，$\lambda_0=1$，而当 $k\geqslant1$ 时，

$$\lambda_k=\sum_{n=0}^{k}p^n g_p^{(n)},\ k\geqslant1,$$

这里

$$g_p^{(n)}=\begin{cases}1, & \text{如 } 0\leqslant n\leqslant\omega;\\ p^{n-\omega}, & \text{如 } n\geqslant\omega.\end{cases}$$

(2) 对Dirichlet级数

$$J_p(s)=\sum_{k=0}^{\infty}\frac{\lambda_k}{p^{ks}},\ \mathrm{Re}\ s>3,$$

有

$$J_p(s)=(1-\lambda)^{-1}(1-p^2\lambda)^{-1}\cdot\begin{cases}1 & ,\text{如 }\omega=0;\\ \left(1-(p-1)\sum\limits_{n=1}^{\omega}(p\lambda)\right)^n, & \text{如}\omega\geqslant 1,\end{cases}$$

这里 $\lambda=p^{-s}$。

推论 AAC猜想等价于 $J_p(s)$ 是 $P^1(F_{p^2})$ 的Zeta函数。

定理3.2的证明 对一个非负整数 k，令

$$T\left(p^k;\frac{2}{\sqrt{p}}\right)=\sum_{w(\bmod p^k)}\Psi\left(\frac{w+\frac{2}{\sqrt{p}}}{p^k}\right).$$

我们先来证明下面的命题。

命题 对一个非负整数 k，我们有

$$T\left(p^k;\frac{2}{\sqrt{p}}\right)=\mu_k\Psi(2\sqrt{p}),$$

$$(T(p^k)\Psi)(2\sqrt{p})=\lambda_k\Psi(2\sqrt{p}),$$

这里

$$\mu_k=p^kg_p^{(k)},\ \lambda_k=\sum_{n=0}^{k}\mu_n=\sum_{n=0}^{k}p^ng_p^{(n)},\ k\geqslant 0.$$

命题的证明 首先由定理3.1及其推论的证明（即(7.26)）有：

$$\lambda_0=1,\ \lambda_1=1+pg_p^{(1)},\ \mu_0=1,$$

其次区别 $p\equiv 1(\bmod 8)$ 与 $p\equiv 5(\bmod 8)$ 两种情况，不难证明

$$J(16p^{2k+1};16p)=g_p^{(k)},\ k\geqslant 0. \tag{7.27}$$

由此易得

$$J(16p^{2k+1};\ 16p^{2l+1})=\frac{g_p^{(k)}}{g_p^{(l)}},\ \text{如 }0\leqslant l\leqslant k, \tag{7.28}$$

在定理2.2中，取 $A=1$，$B=0$，$C=4p$，$N=p^k$，$k\geqslant 2$，则有 $D=16p$，$\alpha=2\sqrt{p}$。

易知两个满足 $m+n=k$ 与 m，$n\geqslant 0$ 的整数 m，n 有

$$g.c.d.(p^{2m},\ 2p^m w,\ w^2-4p^{2n+1})$$
$$=\begin{cases}1, \text{如 } m=0 \text{ 或 } p\nmid w;\\ p, \text{如 } p|w, \text{且 } n=0,\ m=k;\\ p^2 g.c.d.(p^{2(m-1)},\ 2p^{m-1}w_1,\ w_1^2-4p^{2(n-1)+1}),\\ \text{如 } p|w,\ w_1=\dfrac{w}{p}, \text{且 } n,\ m\geqslant 1.\end{cases}$$

这样由定理 2.2 与(7.27)可得

$$\sigma(p^k)g_p^{(k)}\Psi(2\sqrt{p})=(T(p^k)\Psi)(2\sqrt{p})$$
$$+(J(16p^{2k+1};16p^{2k-1})-1)T\left(p^{k-1};\frac{2}{\sqrt{p}}\right)$$
$$+J(16p^{2k+1};16p^{2k-3})\sigma(p^{k-2})J(16p^{2k-3};16p)$$
$$\Psi(2\sqrt{p})-(T(p^{k-2})\Psi)(2\sqrt{p}),$$

从而再用(7.28)即有

$$(T(p^k)\Psi)(2\sqrt{p})=(T(p^{k-2})\Psi)(2\sqrt{p})$$
$$+(p^k+p^{k-1})g_p^{(k)}\Psi(2\sqrt{p})$$
$$+\left(1-\frac{g_p^{(k)}}{g_p^{(k-1)}}\right)T\left(p^{k-1};\frac{2}{\sqrt{p}}\right), \text{如 } k\geqslant 2. \tag{7.29}$$

再在定理 2.2 中，取 $A=p$, $B=0$, $C=4$, $N=p$, 即可得出

$$T\left(p;\frac{2}{\sqrt{p}}\right)=pg_p^{(1)}\Psi(2\sqrt{p}), \tag{7.30}$$

最后，在定理 2.2 中，取 $A=p$, $B=0$, $C=4$, $N=p^k$, $k\geqslant 2$, 并注意到：对两个整数 m, $n=k-m\geqslant 0$ 有

$$g.c.d.(p^{2m+1},\ 2p^{m+1}w,\ pw^2-4p^{2n})$$
$$=\begin{cases}1, \text{如 } n=0;\\ p, \text{如 } n=k \text{ 或 } n,\ m\geqslant 1 \text{ 而 } p\nmid w,\\ p^2 g.c.d.(p^{2(m-1)+1},\ 2p^{(m-1)+1}w_1,\ pw_1^2-4p^{2(n-1)}),\\ \text{如 } n,\ m\geqslant 1,\ p|w,\ w=pw_1.\end{cases}$$

则可得

$$\sigma(p^k)J(16p^{2k+1};16p)\Psi\left(\frac{2}{\sqrt{p}}\right)=T\left(p^k;\frac{2}{\sqrt{p}}\right)$$
$$+J(16p^{2k+1};16p^{2k-1})(T(p^{k-1})\Psi)(2\sqrt{p})$$

$$+J(16p^{2k+1};16p^{2k-3})\sigma(p^{k-2})J(16p^{2k-3};16p)\Psi\left(\frac{2}{\sqrt{p}}\right)$$
$$-J(16p^{2k+1};16p^{2k-1})(T(p^{k-3})\Psi)(2\sqrt{p})$$
(当 $k=2$ 时，这项为 0)
$$-J(16p^{2k+1};16p^{2k-1})T\left(p^{k-2};\frac{2}{\sqrt{p}}\right),$$

由此及 (7.26)、(7.28)，得出

$$\begin{aligned}T\left(p^k;\frac{2}{\sqrt{p}}\right)=&\frac{g_p^{(k)}}{g_p^{(k-1)}}T\left(p^{k-2},\frac{2}{\sqrt{p}}\right)\\&+(p^k+p^{k-1})g_p^{(k)}\Psi(2\sqrt{p})\\&-\frac{g_p^{(k)}}{g_p^{(k-1)}}(T(p^{k-1})\Psi)(2\sqrt{p})\\&+\frac{g_p^{(k)}}{g_p^{(k-1)}}(T(p^{k-3})\Psi)(2\sqrt{p}),\end{aligned}\tag{7.31}$$

其中当 $k=2$ 时，最后一项为 0。

由证明的开头所述及(7.30)可知，对 $k=0, 1$ 命题已真，即已证明 $\lambda_0=1$, $\lambda_1=pg_p^{(1)}+1$, $\mu_0=1$, $\mu_1=pg_p^{(1)}$。我们对 $k\geqslant 2$, 来用归纳法，由归纳假设及(7 29)与(7.31)可得，当 $k\geqslant 2$ 时，有：

$$\begin{aligned}\mu_k&=\frac{g_p^{(k)}}{g_p^{(k-1)}}(\mu_{k-2}-\lambda_{k-1}+\lambda_{k-3})+(p^k+p^{k-1})g_p^{(k)}\\&=\frac{g_p^{(k)}}{g_p^{(k-1)}}(p^{k-2}g_p^{(k-2)}-p^{k-1}g_p^{(k-1)}-p^{k-2}g_p^{(k-2)})\\&\quad+(p^k+p^{k-1})g_p^{(k)}=p^kg_p^{(k)},\end{aligned}$$

与

$$\begin{aligned}\lambda_k&=\lambda_{k-2}+\left(1-\frac{g_p^{(k)}}{g_p^{(k-1)}}\right)\mu_{k-1}+(p^k+p^{k-1})g_p^{(k)}\\&=\sum_{n=0}^{k-2}p^ng_p^{(n)}+\left(1-\frac{g_p^{(k)}}{g_p^{(k-1)}}\right)p^{k-1}g_p^{(k-1)}+(p^k+p^{k-1})g_p^{(k)}\\&=\sum_{n=0}^{k}p^ng_p^{(n)},\end{aligned}$$

这就证明了命题在 k 时也成立，由归纳法，命题已真。

定理 3.2 证明的继续　定理 3.2 的第一个断言，由命题立刻可得。由此可知：

$$
\begin{aligned}
J_p(s) &= \sum_{k=0}^{\infty}\frac{\lambda_k}{p^{ks}} = \sum_{k=0}^{\infty}p^{-ks}\sum_{n=0}^{k}p^n g_p^{(n)} = \sum_{n=0}^{\infty}p^n g_p^{(n)}\sum_{k\geq n}^{\infty}p^{-ks} \\
&= (1-p^{-s})^{-1}\sum_{n=0}^{\infty}g_p^{(n)}p^{-n(s-1)} \\
&= (1-p^{-s})^{-1}\Big(\sum_{0<n<\omega}p^{-n(s-1)} + \sum_{n>\omega}^{\infty}p^{n-\omega}p^{-n(s-1)}\Big) \\
&= (1-p^{-s})^{-1}\big((1-p^{-\omega(s-1)})(1-p^{-(s-1)})^{-1} \\
&\quad + p^{-\omega(s-1)}(1-p^{-(s-2)})^{-1}\big) \\
&= (1-\lambda)^{-1}(1-p^2\lambda)^{-1}\cdot\begin{cases}1, & \text{如 } \omega=0; \\ 1-(p-1)\sum\limits_{n=1}^{\omega}(p\lambda)^n, & \text{如} \omega\geqslant 1,\end{cases}
\end{aligned}
$$

其中 $\lambda=p^{-s}$。定理证毕。

推论的证明是显然的。

附注 如果我们能证明 $J_p(s)$ 是有限域 F_{p^s} 上的一个绝对非奇异射影流形的 Zeta 函数，则由 A. Weil-P. Deligne 定理，就证明了 AAC 猜想的真实性，所以上述的论述指出了 AAC 猜想研究的一个可能的途径。

§4 Mordell 猜想与 Hirzebruch 和

在本节中，我们给出与 §3 的定理 3.1 和定理 3.2 类似的两个定理。

定理 4.1 设有理素数 $p\equiv 3 \pmod 4$，$\alpha=\dfrac{b+\sqrt{p}}{a}$，其中 a，b 为有理整数，且满足

$$a>0,\ p\nmid a,\ a\mid p-b^2.$$

那么，我们有

$$(T(p)\Psi)(\alpha)=((p+2)g_p-1)\Psi(\alpha),\ T(p)=pT_1(p),$$

这里 $T_1(p)$ 为(7.11)定义的 Hecke 算子；

$$g_p=\begin{cases}1, & \text{如 } p\mid u; \\ p, & \text{如 } p\nmid u,\end{cases}$$

其中已设实二次域 $\mathbf{Q}(\sqrt{p})$ 的基本单位为

$$\varepsilon = t + u\sqrt{p}.$$

证明　完全与定理 3.1 的证明类似。

推论　如对一个素数 $p \equiv 3 \pmod 4$，Mordell 猜想成立，则有

$$\Psi(p\sqrt{p}) = (p+2)\Psi(\sqrt{p}).$$

证明　与定理 3.1 的推论的证明完全类似。

定理 4.2　对一个素数 $p \equiv 3 \pmod 4$，令实二次域 $Q(\sqrt{p})$ 的基本单位为 $\varepsilon = t + u\sqrt{p}$，非负整数 ω 由下式定义：

$$p^{\omega} \| u.$$

则有：

(1) 对任一个非负整数 k，有

$$(T(p^k)\Psi)(\sqrt{p}) = \lambda_k \Psi(\sqrt{p}), \quad T(n) = nT_1(n),$$

这里 $T_1(n)$ 由 (7.11) 定义，$\lambda_0 = 1$，而对 $k \geqslant 1$，有

$$\lambda_k = \sum_{n=0}^{k} (-1)^{k-n} \frac{p^{n+1} + p^n - 2}{p-2} g_p^{(n)},$$

其中

$$g_p^{(n)} = \begin{cases} 1, & \text{如 } 0 \leqslant n \leqslant \omega; \\ p^{n-\omega}, & \text{如 } n \geqslant \omega. \end{cases}$$

(2) 对 Dirichlet 级数

$$J_p(s) = \sum_{k=0}^{\infty} \frac{\lambda_k}{p^{ks}}, \quad \mathrm{Re}\, s > 3,$$

有

$$J_p(s) = (1+\lambda)^{-1}(1-p\lambda)^{-1}(1-p^2\lambda)^{-1}$$

$$\cdot \begin{cases} (1 + p\lambda), & \text{如 } \omega = 0; \\ (1 - (p^2-2)\lambda + (p^3 - p^2)\lambda^2), & \text{如 } \omega = 1; \\ \left(1 - (p^2-2)\lambda - 2(p^2-1)\sum_{j=2}^{\omega} \lambda^j \right. \\ \left. \quad + p^2(p^{\omega} + p^{\omega-1} - 2)\lambda^{\omega+1}\right), & \text{如 } \omega \geqslant 2. \end{cases}$$

这里 $\lambda = p^{-s}$。

证明　与定理 4 的证明完全类似，这里不再赘述。

本 章 评 注

1. Ankeny-Artin-Chowla 和 Mordell 关于 Pell 方程的两个猜想提出至今已有三十多年的历史，但至今仍无从下手。本章所提供的事实说明了这两个猜想与 Hirzebruch 和在 Hecke 算子作用下的特征值有密切关系，有点类似于Hecke尖点形式在Hecke算子作用的特征值与 Fourier 系数的关系。因此这两个猜想在某种程度上与 Petersson-Ramanujan 猜想有点类似。后者已在很多情况下由 P.Deligne 证明，他是基于他所证明的 A.Weil 猜想而得到的。因此能否借鉴这一点是令人感到兴趣的。

2. 有关的结果，取自参考文献[63—67]。

3. Petersson-Knopp 恒等式的证明引自参考文献[40]。

参考文献

[1] Ankeny N C, Artin E and Chowla S.The class number of real quadratic number fields.Ann.Math.1952: 56(2), 479-493

[2] Ankeny N C. Chowla S and Hasse H. On the class-number of the maximal real subfield of a cyclotomic field.J.reine Angew. Math.1965, 217: 217-220

[3] Baker A. Transcendental Number Theory. Cambridge University Press. 1975

[4] Baker A and Masser D W. Transcendence theory. Advances and Applications (Edited) Academic Press: London, New York and San Francisco, 1977

[5] Birch B J and Swinnerton-Dyer H P F. Notes on elliptic curves J.Reine Angew.Math.1965, 218: 79-108

[6] Borevich Z I and Safarevich I R Number Theory. Academic Press: London and New York, 1966

[7] Buhler J P, Gross H and Zagier D. On the Conjecture of Birch and Swinnerton-Dyer for an Elliptic Curve of Rank 3.Math.Comp, 1985, 44: 473-481

[8] Burgess D A On character sums and L-series. II. Proc. London Math. Soc 1963, 3(13): 524-536

[9] Cassels J. Rational Quadratic Forms. Academic Press: London, New York and San Francisco, 1978

[10] Chowla S and Friedlander J. Class numbers and quadratic residues.Glasgow Math.J.1976, 17: 47-52

[11] Cohn H. Advanced Number Theory. Dover Publications, Inc New York, 1962

[12] Davenport H. Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields.Proc.London Math.Soc.1951, 2(53): 65-82

[13] Deuring M. Imaginar-quadratischer Zahlkorper mit der Klassenzahl (1), Math.Z.1933, 37: 405-415

[14] Edwards H M. Riemann's Zeta Function. Academic Press: New York, San Francisco and London, 1974

[15] Ennola V. On the first inhomogeneous minimum of indefinite binary quadratic forms and Euclid's algorithm in real quadratic fields.Ann.Univ.Turku.Ser.A I 1958, 28

[16] 冯克勤。代数数论入门。上海：上海科学技术出版社，1988

[17] 冯克勤，陆洪文. Some Development on Algebraic Number Theory in China, Advances in Math.1992, V.20, 56-78

[18] Flath D E. Introduction to Number Theory. John Wiley & Sons: New York, Chichester, Brisbane, Toronto and Singapore, 1989

[19] Gauss C F.Disquisitiones arithmeticae.1801

[20] Gradshteyn I S and Ryzhik L M. Table of integrals, series, and Products Academic Press: New York, London, Toronto, Sydney and San Francisco, 1980

[21] Goldfeld D M. A simple proof of Siegel's theorem. Proc. Nat. Acad.Sci.U.S.A.1974, 71: 1055

[22] Goldfeld D M. The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer. Ann. Scuola Norm. Sup.Pisa 1976, 4(3): 623-663

[23] Gross B and Zagier D. Points de Heegner et derivees de fonctions L.C.R.Acad.Sci.Paris.1983, 297: 85-87

[24] Gross B and Zagier D.Heegner points and derivatives of L-series. Invent. Math. 1986, 84: 225-320

[25] Hardy G H and Wright E M. An Introduction to the Theory of Numbers. Clarendon Press.Oxford, 1954

[26] Hasse H.Bewes analogous der Riemannschen Vermutung fur die Artinsche und F. K. Schmidtschen Kongruenz-zetafunktionen in gewisse elliptischen Fallen.Nachr.Akad. Wiss. Gottingen 1933, 253-262

[27] Heath-Brown D R Hybrid bounds for Dirichlet L-functions II. Quart.J.Math.Oxford 1980, 2(31): 157-167

[28] Hecke E. Lectures on the Theory of Algebraic Numbers. GTM 77. Springer-Verlag: New York, Heidelberg and Berlin, 1981

[29] Heegner K. Diophantische Analysis und Modulfunktionen. Math.Z. 1952, 56: 227-253

[30] Heilbronn H. On the class number in imaginary quadratic fields. Quart.J.Math.Oxford Ser.1934, 25: 150-160

[31] Heilbronn H and Linfoot E H. On the imaginary quadratic corpora of class number one.Quart.J.Math.Oxford Ser.1934, 25: 293-301

[32] Hickerson D J. Continued fractions, and density results for Dedekind sums.J.Reine Angew.Math.1977, 290: 113-116

[33] Hirzebruch F and Zagier D. Classification of Hilbert Modular Surfaces.in: Complex Analysis and Algebraic Geometry. A Collection of Papers Dedicated to K.Kodaira (edited by W.L.Baily, Jr. and T.Shioda). Iwanami Shoten, Publishers and Cambridge Univ-

ersity Press, 1977

[34] Hoffstein J.On the Siegel-Tatuzawa theorem. Acta Arith. 1980, 38: 189-192

[35] 华罗庚. 数论导引. 北京: 科学出版社, 1957

[36] Hua L K. On the distribution of quadratic non-residues and the Euclidean Algorithm in real quadratic fields.I. Trans. Amer. Math. Soc.1944, 56: 537-546

[37] Hua L K and Min S H. On the distribution of quadratic non-residues and the Euclidean Algorithm in real quadratic fields II. Trans.Amer.Math.Soc.1944, 56: 547-569

[38] Husemoller D.Elliptic Curves.GTM 111.Springer-Verlag.New York, 1987

[39] Ireland K and Rosen M. A Classical Introduction to Modern Number Theory. GTM 84. Springer-Verlag: New York, Heidelberg and Berlin, 1982

[40] Knopp M I. Hecke Opertors and an Identity for the Dedekind Sums.J.Number Theory.1980, 12: 2-9

[41] Koblitz N. Introduction to Elliptic Curves and Modular Forms. GTM 97.Springer-Verlag: New York, Heidelberg and Berlin, 1984

[42] Lachaud G.On real quadratic fields.Bull.Amer.Math.Soc. 1987, 17: 285-295

[43] Landau E.Uber die Klassenzahl imaginar-quadratischer Zahlkorper Gottinger Nachr.1918, 285-295

[44] Lang S Introduction to Modular Forms. Springer-Verlag: Berlin, Heidelberg and New York, 1976

[45] 陆洪文. 循环连分数的一个注记. 中国科大学报. 1975, 5(2): 83-88

[46] 陆洪文. 关于实二次域的类数. 科学通报. 1979, 24(4): 149-150

[47] 陆洪文. On the class-number of real quadratic fields, Scientia Sinica, special issue(II)on Math.1979, 118-130

[48] 陆洪文. 类数为1的实二次域. 中国科大学报, 1980, 10(4): 133-135

[49] 陆洪文. On the real quadratic fields with class-number one.Scientia Sinica, 1981, V.24: 1352-1357

[50] 陆洪文. Congruences for the class number of quadratic fields. Abh. Math.Sem.Univ.Hamburg 1982, 52: 254-258

[51] 陆洪文. On real quadratic fields with class number one. A Monthly Journal of Science, 1983, 28(1): 134-135

[52] 陆洪文. The continued fractions, class number and the others. Scientia Sinica (A)1983, V.26: 1276-1284

[53] 陆洪文. Kronecker limit formula of real quadratic fields(I)Scientia Sinica(A)1984, V.27: 1233-1250

[54] 陆洪文. 实二次无理数连分数展开式周期的长度. 数学学报, 1986, 29: 433-443

[55] 陆洪文. A. Kronecker limit formula and its applications. IHES/M/86/25

[56] 陆洪文. Fibonacci numbers, continued fractions and the class number of quadratic fields. IHES/M/86/32

[57] 陆洪文. A note on Goldfeld-Gross-Zagier-Oesterle theorem. IHES/M/86/39

[58] 陆洪文. Pellian equation, continued fractions and class number of the quadratic fields (in Chinese) Research Report of the Institute of Math. Academia Sinica, 1987, 37-40

[59] 陆洪文. Transformation of Dedekind η function, Acta Math. Scientia 1988, 8(3): 249-262

[60] 陆洪文, 张明尧. Kronecker limit formula for real quadratic fields(II) Sci. Sinica(A) 1989, 32: 1409-1422

[61] 陆洪文. On the value at -1 of the zeta functions for the ambiguous ideal of real quadratic fields J. Sichuan Univ. Natural Science Edition special issue 1989/1990, V. 26: 66-71

[62] 陆洪文. Hirzebruch sum and class number of the quadratic fields Chin. Sci. Bull. 1991, V. 36: 1145-1147

[63] 陆洪文. Hecke operator and pellian equation conjecture(I). in "International Symposium in Memory of Hua Loo Keng" 1991, Number Theory 183-191, Springer-Verlag

[64] 陆洪文. Hecker operators and Hirzebruch sums, J. N. T. 1991, 38: 185-195

[65] 陆洪文. Hecke operators, Hirzebruch sums and Pellian equation conjectures to appear in Proc. of Nakai Math. Institute, 1990

[66] 陆洪文. Hecke operator and Pellian equation conjecture (II), Chin. Ann of Math. 1991, 13B(4): 46-53

[67] 陆洪文. Hecke operator and Pellian equation conjecture (III), Syst. Soi. & Math. 1991, V. 4: 97-103

[68] 陆洪文, 张明尧, S. Chowla's conjecture on a class of real quadratic fields (Preprint)

[69] 陆洪文, 张明尧. On the analytic continuation and the funcitional equation for a kind of L-functions for real quadradic fields (Preprint)

[70] 陆洪文, 裴定一. Modular forms with weight 3/2 and class number of quadratic fields. Preprint of the Institute of Math., Academia Sinica, Beijing, China

[71] 陆洪文, 计光恒. Class number and computer (Preprint 1991)

[72] Mazur B. Modular curves and the Eisenstein ideal. IHES Publ Math.1978, 47: 33-186

[73] Mazur B and Swinnerton-Dyer H. Arithmetic of Weil curves. Invent.Math.1974, 25: 1-61

[74] Mollin R A. Diopantine Equations and Class Numbers, J. Number Thy.1986, 24: 7-19

[75] Mollin R A. On the Insolubility of a Class of Diophantine Equations and the Nontriviality of the Class Numbers of Related Real Quadratic Fields of Richaud-Degert Type. Nagoya.1987, J.105: 39-45

[76] Mollin R A.Necessary and Sufficient Conditions for the Class Number of a Real Quadratic Field to be One, and a Conjecture of S.Chowla.Proc.Amer.Math.Soc.1988, 102: 17-21

[77] Mollin R A. Class Number One Criteria for Real Quadratic Fields I.Proc.Japan Acad.Ser.1987, A.63: 121-152

[78] Mollin R A. Class Number One Criteria for Real Quadratic Fields II.Proc.Japan Acad.Ser.1987, A.63: 162-164

[79] Mollin R A and Williams H C. A Conjecture of S. Chowla Via the Generarilized Riemann Hypothesis. Proc. Amer. Math. Soc. 1988, 102: 794-796

[80] Mollin R A and Williams H C. Class number one for real quadratic fields, continued fractions and reduced ideals. Number Theory and Applications (ed.R.A.Mollin) (NATO ASI series). vol. C265.Kluwer Academic Publishers, Berlin, New York. 1989. pp. 481-496

[81] Mordell L J. On the Riemann hypothesis and imaginary quadratic fields with a given class number.J.London Math. Soc. 1934, 9: 289-298

[82] Mordell L J.On the rational solutions of the indeterminate equations of the 3rd and 4th degrees. Proc. Camb. Phil. Soc. 1922, 21: 179-192

[83] Mordell L J. On the Pellian equation conjecture(II). J. London Math.Soc. 1961, 36: 282-288

[84] Oesterle J. Nombres de class des corps quadratiques imaginaires. Sem.Bourbaki, 1983-1984, Exp.631

[85] Ogg A P.On a convolution of L-series. Invent.Math. 1969, 7: 297-312

[86] 潘承洞,潘承彪. 解析数论基础. 北京: 科学出版社, 1991

[87] Perron O.Die Lehre von Kettenbruchen.Teubner, Stuttgart. 1954

[88] Rabinovitch, G.Eindeutigkeit der Zerlegung in Primzahlfaktoren in

quadratischen Zahlkorpern. Proc. Fifth Internat Congress Math. (Cambridge) 1913, Vo. I: 418-421

[89] Rademacher H.Topics in Analytic number theory.Springer-Verlag: Berlin, 1971

[90] Shimura G. Introduction to the arithmetic theory of automorphic functions.Iwanami Shoten and Princeton University Press, 1971

[91] Shimura G. On the holomorphy of certain Dirichlet series. Proc. of the London Math.Soc.1975, 31: 79-98

[92] Siegel C L. Über die Classenzahl quadratischer Zahlkörper. Acta Arith. 1935, 1: 83-86

[93] Siegel C L. Berechnung von Zetafunktionen an ganzzahligen Stellen.Nachr.Akad Wiss.Gottingen.1969, Nr.10: 80-102

[94] Silverman J H. The Arithmetic of Elliptic Curves. GTM 106. Springer-Verlag: New York, Heidelberg and Berlin, 1986

[95] Stark H M. On the complex quadratic fields with class number equal one.Trans.Amer.Math.Soc.1966, 122: 112-119

[96] Stark H M. A complete determination of the complex quadratic fields of class-number one.Michigan Math.1967, J.14: 1-27

[97] Stark H M. A historical note on complex quadratic fields with class number one.Proc.Amer.Math.Soc.1969, 21: 254-255

[98] Stark H M. On the 'gap' in a theorem of Heegner. J. Number Theory 1969, 1: 16-27

[99] Stark H M. A transcendence theorem for class number problems. Ann.of Math.1971, 2(94): 153-173

[100] Stark H M. Some Effective Cases of the Brauer-Siegel Theorem. Invent.Math.1974, 23: 135-152

[101] Swinnerton-Dyer H P F and Birch J. Elliptic curves and Modular functions.in: Modular Functions of One Variable IV.Lect. Notes in Math. 476. Springer-Verlag: Berlin, Heidelberg And New York, 1972

[102] Tate J.The Arithmetic of Elliptic Curves. Invent. Math. 1974, 23: 179-206

[103] Tatuzawa T.On a theorem of Siegel.Japan.J. math. 1951, 21: 163-178

[104] Titchmarsh E C. The Theory of the Riemann Zeta-Function. Second edition Revised by Heath-Brown. Clarendon Press, Oxford, 1986

[105] Vigneras M F. Valeur au centre de symetrie des fonctions L associees aux formes modulaires. Sem. Delange-Pisot-Poitou, Birkhauser, 1979-80

[106] Waldspurger J L. Correspondances de Shimura et quaternions. (preprint)

[107] Washington L C. Introduction to Cyclotomic Fields. GTM 83. Springer-Verlag: New York, Heidelberg and Berlin, 1982

[108] Watson G L. Integral quadratic forms. Cambridge University Press, 1960

[109] Weil A. Sur un theoreme de Mordell. Bull. Sci. Math. 1930, 2(54): 182-191

[110] Weil A. Sur les fonctions algebriques a corps de constantes fini. C.R.Acad.Sci.Paris 1940, 210: 592-594

[111] Weil A. Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichung. Math. Ann. 1967, 168: 149-156

[112] Yokoi H. Class-number one problem for certain kind of real quadratic fields. Proc. Int. Conf. on Class Numbers and Fundamental Units of Algebraic Number Fields. 24-28 June, Katata, Japan, 1988. 125-137

[113] Zagier D. A Kronecker Limit Formula for Real Quadratic Fields. Math.Ann. 1975, 213: 153-184